United States Patent [19]

Serpell

[11] **Patent Number:** **4,633,037**

[45] **Date of Patent:** **Dec. 30, 1986**

[54] **GENERATION OF IDENTIFICATION KEYS**

[75] Inventor: **Stephen C. Serpell, Ipswich, England**

[73] Assignee: **British Telecommunications public limited company, London, England**

[21] Appl. No.: **581,898**

[22] Filed: **Feb. 21, 1984**

[30] **Foreign Application Priority Data**

Feb. 22, 1983	[GB]	United Kingdom	8304876
Feb. 22, 1983	[GB]	United Kingdom	8304877

[51] **Int. Cl.⁴** **H04L 9/00**

[52] **U.S. Cl.** **178/22.14**; 178/22.16; 178/22.09

[58] **Field of Search** 178/22.08, 22.09, 22.16, 178/22.14

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,798,605	3/1974	Feistel .	
4,193,131	3/1980	Lennon et al.	178/22.09
4,264,782	4/1981	Konheim	178/22.09
4,302,810	11/1981	Bouricius et al.	178/22.16
4,349,695	9/1982	Morgan et al.	178/22.09
4,423,287	12/1983	Zeidler	178/22.08

FOREIGN PATENT DOCUMENTS

002580	of 0000	European Pat. Off. .
029894	of 0000	European Pat. Off. .
089087	of 0000	European Pat. Off. .
082958	of 0000	European Pat. Off. .

OTHER PUBLICATIONS

Proceedings of the National Electronics Conference, vol. 35, Oct. 1981; pp. 309–314, Oak Brook, Illinois, U.S. S. M. Matyas et al: "*Cryptographic Authentication Techniques in PIN-Based Electronic Funds Transfer Systems*" p. 310, line 27, p. 311, line 1.

Seventeenth IEEE Computer Society International Conference, 5th, 8th Sep. 1978, Washington, D.C. pp. 351–354, NY, U.S. M. Sendrow: "*Key Management in EFT Networks*" p. 352, left hand column, lines 14–25: right hand column, lines 11–16; p. 353 left hand column, lines 45–49.

IBM Technical Disclosure Bulletin, vol. 22, No. 12, May 1980, p. 5281, New York, U.S. M. L. Martin: "*Data Encryption in a Multi-Terminal System*" p. 5281.

1978 National Telecommunications Conference, vol. 2, Dec. 1978, pp. 26.1.1.-26.1.6., New York U.S. R. E. Lennon, et al: "*Cryptographic Key Distribution Using Composite Keys*" p. 26.1.2. left-hand column, lines 11-34.

Primary Examiner—Salvatore Cangialosi

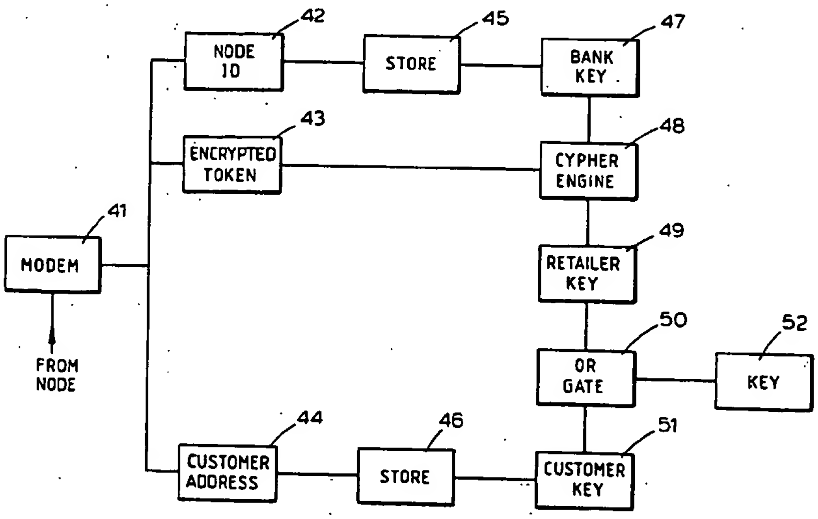
Assistant Examiner—Aaron J. Lewis

Attorney, Agent, or Firm—Nixon & Vanderhye

[57] **ABSTRACT**

Commercial transactions conducted over a telecommunications link are verified using a transaction key available at both ends of the link. The transaction key is produced by combining (1) data supplied to the retailer by a customer and stored by the bank with (2) data stored by the retailer. The telecommunications link includes a node which passes the retailer's data to the bank in the form of a label obtained by encrypting the retailer's code with a client code. The bank retrieves the bank code and decrypts the label to obtain the retailer's code. The bank also retrieves the customer's data and combines the two elements to obtain the same transaction key that was created at the retailer's terminal.

14 Claims, 4 Drawing Figures



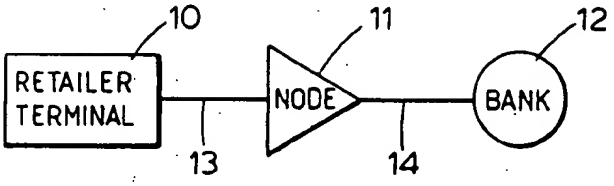

10
11
12
RETAILER TERMINAL
NODE
BANK
13
14

Fig.1

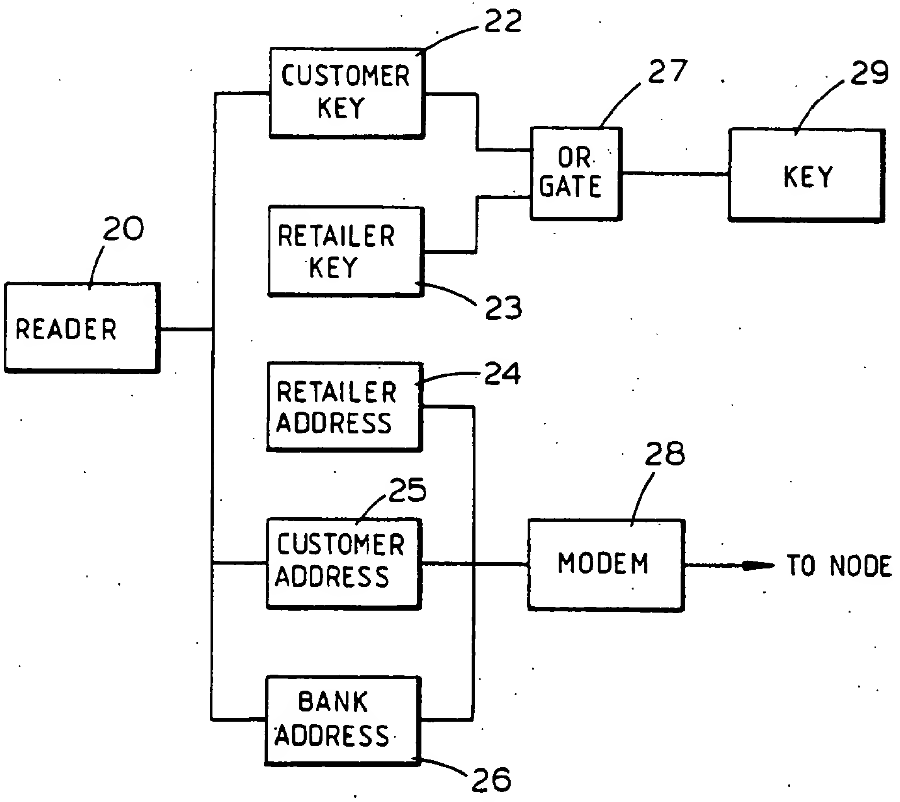

22
CUSTOMER KEY
27
29
OR GATE
KEY
20
RETAILER KEY
READER
23
RETAILER ADDRESS
24
28
25
CUSTOMER ADDRESS
MODEM
TO NODE
BANK ADDRESS
26

Fig.2

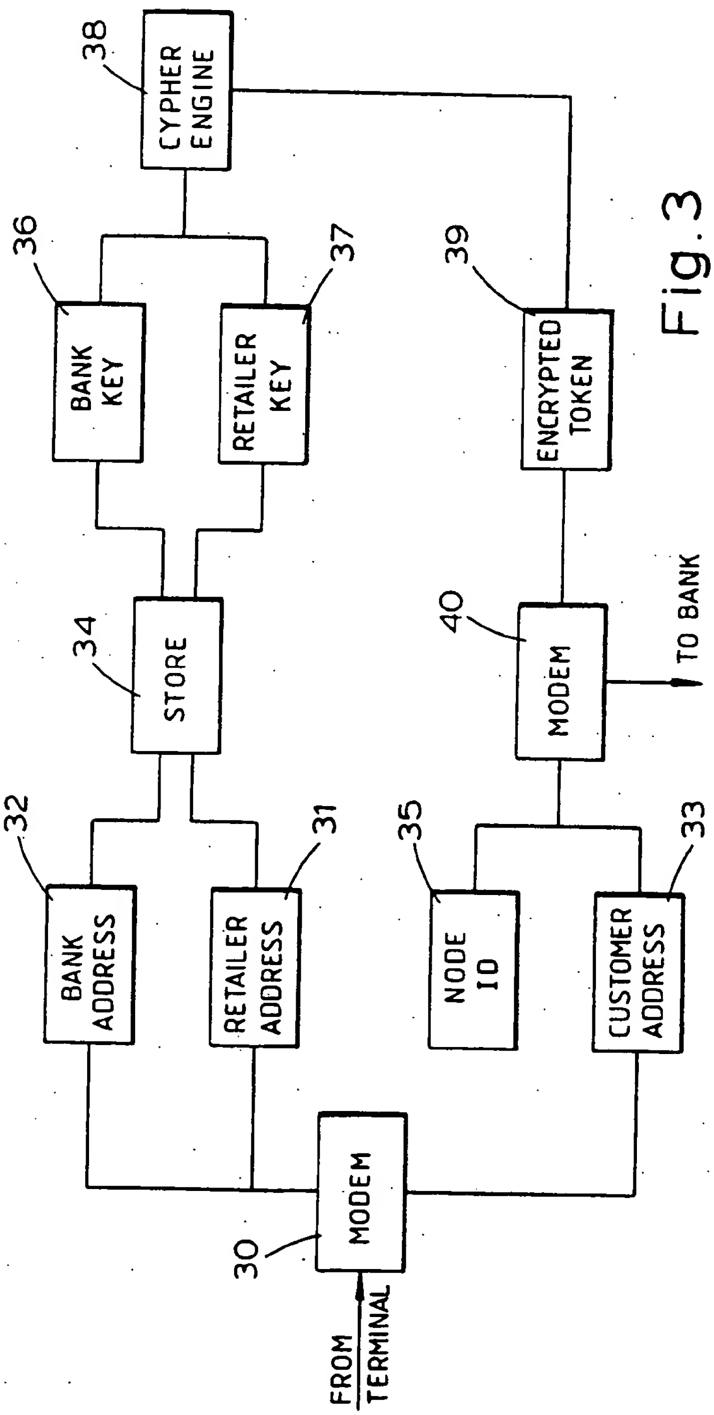

FROM TERMINAL
30
MODEM
32
BANK ADDRESS
31
RETAILER ADDRESS
34
STORE
36
BANK KEY
37
RETAILER KEY
38
CYPHER ENGINE
35
NODE ID
33
CUSTOMER ADDRESS
40
MODEM
TO BANK
39
ENCRYPTED TOKEN

Fig. 3

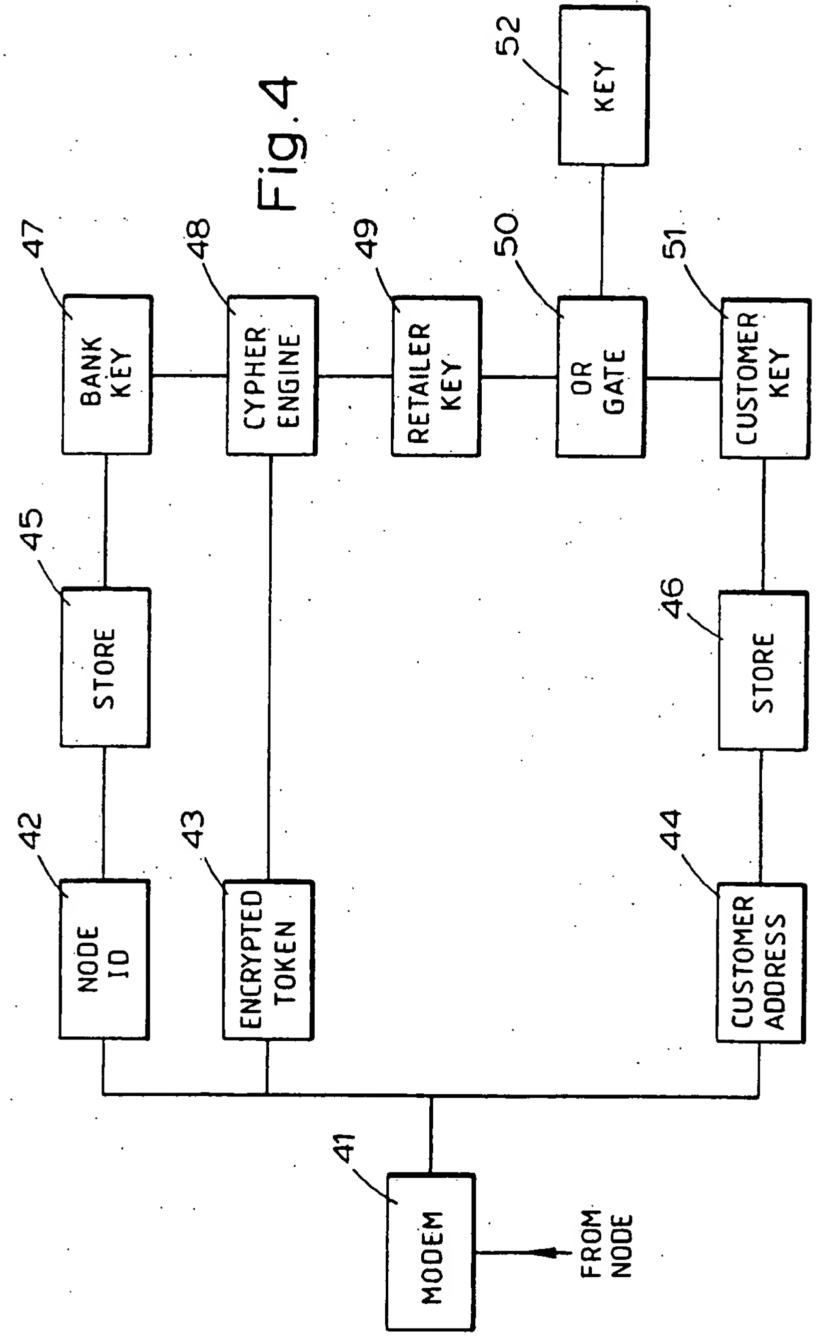


Fig.4
BANK KEY
47
CYPHER ENGINE
48
RETAILER KEY
49
OR GATE
50
CUSTOMER KEY
51
KEY
52
STORE
45
STORE
46
NODE ID
42
ENCRYPTED TOKEN
43
CUSTOMER ADDRESS
44
MODEM
41
FROM NODE

GENERATION OF IDENTIFICATION KEYS

This invention relates to the generation of identification keys and especially identification keys for use in the automatic transfer of funds by telecommunication networks.

This application is related to my copending applicatin Ser. No. 581,897 filed concurrently herewith.

The transfer of funds involves three parties, namely,

(1) the customer

(2) the retailer

(3) the customer's bank

and verifying the identities of the parties is important, e.g. to prevent frauds or other criminal activities. Systems of this nature utilize identification keys which must be kept secret. Two such keys are needed, i.e.

(a) a key known only to the customer and the bank

(b) a key known only to the retailer and the customer's bank.

A large system might include 100 banks and 100,000 retailers. Any one of the retailers must be able to deal with any one of the banks so that the number of possible pairings is the product of 100 and 100,000; i.e. 10^7. Therefore, the system would need 10^7 different secret keys each of which is present at two locations, i.e. a bank and a retailer. Thus there would be 100,000 retailers each with 100 keys and 100 banks each with 100,000 keys.

Such a system is cumbersome to the point of being impractical. It is an object of the present invention to reduce the number of keys without substantially reducing the security.

This invention automatically generates an identification key for use in the automatic verification of a transaction involving the transfer of funds by means of a telecommunications link which includes at least one nodal station contributing to the cryptographic function wherein said link connects a first station to a second station. In a preferred form of the invention there is only one nodal station in the link. The key is generated by combining an identification code acquired at the first station (hereinafter the "acquired code"), e.g. by automatically reading a customer's card, with an identification code stored at a first location (hereinafter the "station code"). The combination is preferably achieved by using an or-gate on corresponding bits of the two identification codes. The same two identification codes are required at a second location whereby the same combination is performed to generate the same identification key at both first and second stations. (The first station is usually a retailer's terminal and the second station is usually the automatic processing equipment of a bank, conveniently referred to as "the bank".)

The acquired code is available at the second location because it is the practice of banks to store data relating to their customers. The first station also acquires the storage address of the acquired code at the second station and this address is passed, via the telecommunications link, to the second station. Thus the second station can retrieve the acquired code from its storage means. For the reasons given above, it is inconvenient to store at every bank all the data stored at all the terminals of all the retailers. Thus the station code is stored at the first station and at a nodal station but not at the second station. According to this invention the station code is passed from the nodal station to the second station by an automatic method wherein each nodal station receives a message from a predecessor station, and transmits a message to a successor station wherein each nodal station:

(a) accesses storage means using as address the identity of its predecessor station to retrieve a predecessor key;

(b) accesses storage means using as address the identity of the successor station to retrieve a successor key;

(c) encrypts the predecessor key as data with the successor key as key to generate a label;

(d) concatenates the label with the received message to generate an extended message which is the message transmitted to the successor station.

The message received at the second station includes a label generated at each nodal station. The second station uses the identity of the last nodal station as address to retrieve the key needed to decrypt the first label. This reveals a key which decrypts another label and the process continues until all the labels are decrypted whereby the key used at the first station is revealed. The second station thus has the two identification codes neded for combination to generate the key.

It is emphasized that the station code is potentially available at any nodal station but an outsider would require knowledge of an appropriate key to decrypt the labels and obtain the station code. However, the key used for the transaction also requires that the acquired code be available. This key is not available at any nodal station (and it is not available to an outsider).

Our corresponding patent application (BT Patent Case 22963) 22963 describes (U.S. application Ser. No. 581,897, filed concurrently herewith) describes an automatic process for confirming identities at two different stations which method comprises:

(a) at the first station:

(i) generating a first verification code by encrypting data with a first identification key available at the first station

(ii) transmitting said first verification code to the second station

(b) at the second station:

(i) receiving said first verification code

(ii) decrypting said first verification code using a first verification key available at the second station

(iii) generating a second verification code by encrypting the de-crypt obtained in (b) (ii) with a second verification key available at the second station

(iv) transmitting said second verification code to the first station;

(c) at the first station:

(i) receiving the second verification code

(ii) utilizing a second verification key available at the first station to confirm that second verification code is derived from the same data as the first verification code.

It is preferred to operate this process and the process of this invention in conjuction. Preferably the two methods are operated simultaneously. To utilize the combination, the "first identification key" specified in (a) (i) is the "identification key" generated by combining the "acquired code" and the "station code" of this invention. The "second verification key" specified in (b) (iii) is also sorted at the second location and acquired at the first location.

In a commercial transaction it is desirable to provide good security for the identification of a customer. It is conventional for persons to carry a card on which is recorded, in machine readable form, identification data. In case the card is lost the owner remembers a "personal identity number" or "PIN" which is provided to a retailer's terminal by means of a key pad. Identification which includes the PIN sometimes fails, even in the absence of fraud, because of human error in entering the PIN.

In the operation of the method according to the invention it is preferred that the "acquired code" uses only data recorded on the card, which has the result that the "identification key" is not affected by human error. The "second verification key", which is retrieved from storage at the second station, preferably depends on the PIN, but the retrieval at the second station depends on an address automatically read from a card. The second station therefore returns a message to the first station which the first station tries to verify using the human-entered PIN.

The process is initiated at the first station, e.g. after a retailer's terminal has acquired the relevant data from a customer. The initiation usually comprises the automatic transmission of a message to a nodal station, said message including:

(a) an identification of the first station;

(b) an identification of the second station;

(c) the address of the acquired code at the second station, and, preferably;

(d) A transaction component, being a definition of the proposed transaction and/or a random element, said transaction component being encrypted with the transaction key generated by combining the acquired code and the station code.

Item (b) is used at each nodal station to select a successor station and set up a telecommunication link thereto. As stated above, item (b) is also used as the address to retrieve the successor key.

The second key station decrypts all the labels and forms the transaction key as described above. It uses the transaction key to decrypt item (d) and verifies that the proposed transaction is permissible. If all is in order, the second station re-crypts the random element with a PIN related key and returns the encrypted message to the first station. The return does not need to pass via the nodal stations; any route set up by the public switched method is suitable. The first station decrypts the returned message and verifies identity using a key derived from the PIN input by a (human) customer on its key pad. This final step may fail because of human error and it is usual to offer the customer a plurality of attempts, e.g. up to four, to correct the error, but all these re-trials involve only the first location. It is clearly desirable that data representations transmitted through the nodal stations should all be produced automatically whereby all transmitted data representations have machine accuracy.

An embodiment of the invention will now be described by way of example with reference to the accompanying drawings in which:

FIG. 1 illustrates one link which is set up for a single transaction.

FIG. 2 illustrates the equipment at the first station, e.g. a retailer's terminal.

FIG. 3 illustrates the equipment at a node, and

FIG. 4 illustrates the equipment at the second station, e.g. at a bank's terminal.

In an extensive fund transfer system, e.g. covering the whole British Isles or the whole of the European Economic Community, there would probaby participate more than 100,000 retailers and more than 100 banks. It would be inconvenient to provide initial direct access from every retailer to every bank since this would require at least 10^7 keys. This invention links the retailer and banks via nodal stations which perform cryptograph functions.

For example, the system could comprise 100 nodal stations each of which can be contacted, via a public switched telecommunications network, by 1000 retailers and 100 (i.e. all) the banks. (This reduces the number of keys from 10^7 to 2×10^5.)

It should be noted that this preferred embodiment utilizes only one nodal station in any one link, and the term "node" will be used to imply a link of this type.

It is emphasized that the stations (i.e. first, second and nodal) communicate via a public switched telecommunications network which sets up the links needed to perform the method of the invention. The network includes switching centres which are included in the links. The switching centres do not contribute to the cryptographic system and the switching centres are not to be identified with nodal stations.

The terminal 10, of a retailer reads a customer's card in reader 20. This identifies the customer and his bank 12. Terminal 10 which has access to node 11 by modem 28, (but not to any of the other 99 nodes in the network) transmits via link 13 this information to node 11 which sets up a connection 14 to bank 12. For verification, a transaction key is generated and this key is known only to terminal 10 and bank 12. It is an important feature that the transaction key is not kown to node 10, or anything else in the circuit except the two ends. Link 13 and connection 14 are provided by a public switched network and, as is conventional, both include one or more switching centres.

The transaction key is generated at terminal 10 and bank 12 from the following information.

(1) Customer data This is information contained on a data card carried by the customer and, optionally, from a personal identification number known to the customer but not on the card. This information is acquired by card reader 20 and/or entered by the customer on a key pad (not shown) and entered therefrom into storage means 22 and 25 comprised in terminal 10. Similar information is also contained in storage means 46 at the bank 12 (but it is not available at node 11.)

(2) Station Key of the Retailer This is a secret key available only at the terminal 10 in store 23 and the node 11 in store 34. The node 11 holds 1000 such keys in storage means 34 and, when a terminal identifies itself, the node retrieves the right key be accessing its storage means 34. The retailer's key is not available at the bank 12.

(3) Bank Key This is a secret key available only at node 11 and bank 12. Each bank holds this key in its own storage means. The bank key is not available at the terminal 10. The bank-store 45 holds a different key for each node; the node-store 34 holds a different key for each bank.

The generation of the transaction key will now be described.

Terminal 10 acquires customer data and the address of the customer's bank from card reader 20. The customer data is placed in stores 22 and 25; the bank's address is placed in store 26. The terminal holds the station key in store 23 and the retailer's identity in store 24.

The customer data, in store 22, is combined with the station key, in store 23; using or-gate 27 on corresponding bits as in one-shot-pad encryption. This produces a transaction key which is stored in store 29 at terminal 10 and which has to be made available at bank 12 without transmission.

The terminal 10 sends, by means of modem 28, a signal to the node 11, which signal contains, in clear and intelligible form, its own identity from store 24, the (alleged) identity of the customer from store 25 and the identity of the customer's bank from store 26. No keys are transmitted; this is an important feature of the system.

The node receives the signal on modem 30 and separates it to hold the retailer's identity in store 31, the bank's identity in store 32 and the customer's identity in store 33.

Random access storage means 34 is addressed using the content of store 31 (i.e. the retailer's identity) to retrieve the retailer's key which is placed in store 37. RAM 34 is also addressed using the content of store 32 to retrieve the bank key which is placed in store 36. Cypher engine 38 uses the content of store 37 (i.e. the retailer key) as data and the content of store 36 (i.e. the bank key) as key to produce an encrypted token which is placed in store 39.

The node concatenates:

(a) the content of store 33 (i.e. the customer's alleged identity);

(b) the content of store 35 (i.e. the identity of the node 11);

(c) the content of store 39 (i.e. the encrypted token); and modem 40 transmits the resulting string to the bank 12.

The bank 12 receives the composite signal on modem 41 and separates it to obtain the following three items:

(a) the alleged identity of the customer, which is stored in store 44;

(b) the identity of the node 11, which is stored in store 42; and

(c) the encrypted token, which is stored in store 43.

These are used in four steps as follows:

STEP I

Item (a) is retrieved from store 44 and used to address the bank's storage means 46 to retrieve customer data (which should be identical with that read at terminal 10) and which is placed in store 51.

STEP II

Item (b) is retrieved from store 42 and used to address the bank's storage means 45 to retrieve a bank key (which should be identical to that used at node 11) and which is placed in store 47.

STEP III

Item (c) is retrieved from store 43 and decrypted by cypher engine 48 using as key the content of store 45. The decrypt (which should be the station key used by node 11) is stored in store 49.

STEP IV

The content of store 49 (i.e. the retailer key generated in step III) is combined with the content of store 51 (i.e. customer data retrieved in step I) in or-gate 50 and the result is stored in store 52. This replicates the process used at terminal 10. This should generate the same transaction key which is stored at terminal 10. As this key is known at both ends, it can be used to validate the transaction.

It will be apparent that any failure to retrieve correct data will cause the sequence to fail and abort the transaction. Any criminal attempt to operate a dishonest sequence would require exact knowledge of all the keys. Therefore keeping the keys secret is an important requirement for a sure and secure operation.

As a modification to enable the system to operate even if node 11 fails, the terminal 10 may have access to an alternative node (not illustrated). This modificaton preferably requires a second key at the terminal.

Encryptions are preferably performed using DES algorithm as described in "FIPS PUB 46" of National Bureau of Standards of Department of Commerce of U.S. Government.

The keys can be used to operate the system described in our pending patent application (BT patent case 22963) U.S. application Ser. No. 581,897, filed concurrently herewith.

The above description is based on a transaction involving a customer, a retailer and the customer's bank wherein communication is via a node in a telecommunication network. It is a feature of the invention that an important part of the verification is assigned to the node. The invention is generally applicable where it is convenient to assign part of the verification to a node or to verify that communication passed via an expected node. Thus the transaction would also involve the retailer's bank and communication would also pass via the node. This part of the transaction could also be verified by the invention, e.g. by replacing "Customer data" (item (1) above) by "Retailer data" available at the retailer's terminal and the retailer's bank (but not at the node).

The description above relates to a preferred embodiment wherein there is only one node between the first and second stations. In certain circumstances it is desirable to utilize a chain of nodal stations, each of which operates as described above, with the key of its predecessor in store 37 and the key of its successor in store 36. The bank decrypts each label in turn and each decryption reveals the key for use in the next step.

A system with 10^7 retailers and 1,000 banks linked via 10,000 nodes would require 10^7 keys for use between nodes and retailers and 10^{10} keys for use between nodes and banks. It is possible to reduce the number of keys by utilizing links with two nodal stations, i.e. retailer nodal stations which communicate primarily with retailers and bank nodal stations which communicate primarily with banks.

Using 10,000 retailer nodal stations and 10 bank nodal stations would reduce the number of keys to 10^7 for use between retailers and retailer nodal stations; 1,000 for use between banks and bank nodal stations and 100,000 between nodal stations.

In use, the first station initiates the processes as described above and sends a message to its retailer nodal station which forms a first label by encryptioning a first key with a second key. The retailer nodal station concatenates the first label and passes on the message to the bank nodal station appropriate to the desired second station. The bank nodal station forms a second label by encrypting the second key with a third key, concatenates the second label with the message and sends it to the second station.

The second station retrieves the third key and decripts the second label to reveal the second key. It then uses the second key to decrypt the first label and reveal the first key. At this point the system proceeds as described above.

It is emphasised that the methods disclosed herein are automatic methods carried out electronically. Reference to "Key", "Data" and "Information" should be construed as representations suitable for automatic processing. Different forms of representation are appropriate in different parts of the method, e.g. electromagnetic or electrical pulses during transmission, magnetisation for storage and voltage or currents for processing elements.

I claim:

1. A method for automatically establishing a transaction key at predetermined first and second stations in a system having a multitude of similar first and second stations joined by means of a telecommunication link and including but a single intermediate or nodal data processing station connected between said predetermined first and second stations, without revealing said transaction key at said nodal station, said method comprising the steps of:

(a) at the predetermined first station

(i) combining first data available at both said predetermined first and second stations with second data available at the first station and the nodal station, to generate the transaction key for use in encrypting further data to be transmitted to said second station,

(ii) transmitting to the nodal station third data identifying the first station, the second station and the address of the first data at the predetermined second station;

(b) at the nodal station

(i) accessing nodal storage means using the identity of the predetermined first station as an address to retrieve pre-stored data corresponding to said second data used in step (a) (i),

(ii) accessing nodal storage means using the identity of the predetermined second station as address to retrieve an encryption key characteristic of said second station,

(iii) producing an encrypted label by encrypting the pre-stored data retrieved in step (b) (i) with the encryption key retrieved in step (b) (ii),

(iv) transmitting to the second station the identity of said nodal station;

(c) at the predetermined second station

(i) accessing storage means located at the second station using the identity of the nodal station as address to retrieve an encryption key characteristic of the predetermined second station,

(ii) decrypting the label with the key retrieved in step (c) (i),

(iii) accessing storage means located at the second location using the address of the first data transmitted from the first station,

(iv) combining the data retrieved in step (c) (iii) with the decrypt from step (c) (ii) in a replication of step (a) (i) to generate said transaction key at said second station;

wherein, in a correct operation of the sequence, the data retrieved in step (c) (iii) is the same as the first data used in step (a) (i), and the decrypt obtained in step (c) (ii) is the same as the second data used in step (a) (i),

whereby the transaction key produced in step (c) (iv) is the same as the transaction key produced in step (a) (i).

2. A method of accoding to claim 1, wherein step (a) (ii) further includes the transmission of data representing the identity of the predetermined first station and additional data being transmission data encrypted with the transaction key code established in step (a) (i), as key.

3. A method according to claim 2, wherein the transmitted data includes a random element.

4. A method according to claim 2, wherein a further step (b) (iv), occurring between steps (b) (iii) and (c) (i), includes transmitting data representing the identity of the nodal station, and forwarding the encryped additional data received from the predetermined first station.

5. A method according to claim 4, wherein the predetermined second station decrypts the encrypted additional data using as key the transaction key generated in step (c) (iv).

6. A method according to claim 5, in which the transaction keys of steps (a) (i) and (c) (iv) are generated by an exclusive-or-gate.

7. A station, adpated to participate in a method according to claim 2, as said predetermined first station and comprising;

(a) input means for acquiring

(i) data representing identification of a second station,

(ii) said first data, and

(iii) data representing an address where the first data is stored at the second station;

(b) storage means operatively connected to the input means for storing the data acquired by the input means;

(c) storage means for storing said second data representing a station code;

(d) combining means for combining the first data and the second data;

(e) concatenating means for producing message data by contatenating the data representing the identity of the second station, the address of the first data at the second station and data representing an identification of the predetermined first station; and

(f) means, operatively connected to the concatenating means, for transmitting the message to a nodal station.

8. A first station according to claim 7, wherein the combining means is an exclusive-or-gate means for accepting and combining the first data and second data as input.

9. A station, adapted to participate in a method according to claim 5 as said predetermined second station and comprising

(a) storage means for storing data representing

(i) the identity of nodal stations properly able to communicate with the second statin, and

(ii) the identity of customers associated with this second station;

(b) retrieval means for accessing the storage means with data representing the identity of a nodal station and retrieving a key associated with this second station;

(c) cypher engine means for decrypting a label using as key the retrieval key of this second station;

(d) retrieval means for accessing the storage means with the data representing the identity of a customer as address to retrieve the first data also used at the first station; and

(e) combining means for combining the locally retrieved first data with the retrieved key of this station to obtain the transaction key.

10. A station according to claim 9, wherein the combining means is an exclusive-or-gate means for accepting the retrieved key of this station obtained from said cypher engine means and the locally retrieved first data from the retrieval means as input.

11. An automatic process for establishing the same cryptographic identification key at first and second stations joined by a telecommunications link which includes a data processing nodal station, said establishment being achieved without revealing said key at said nodal station, which method comprises

(a) at the first station

(i) combining initiation data available at both first and second stations with identification code data available at the first station and said nodal station to generate the identification key;

(iii) transmitting to the nodal station an identification of the first station, of the second station and the address of the initiation data also located in data storage means at the second station;

(b) at said nodal station accessing storage means at the nodal station using the identity of the first station as an address to retrieve identification code data corresponding to that used in step (a) (i) and passing said retrieved code data and the identity of said nodal station to the second station;

(c) at the second station

(i) receiving the retrieved code data retrieved in step (b);

(ii) accessing storage means located at the second location using the address transmitted from the first station to retrieve said initiation data;

(iii) combining the retrieved initiation data retrieved in step (c) (ii) with the retrieved code received in step (c) (i) in a replication of step (a) (i) to locally generate said indentification key at said second station;

wherein, in a correct operation of the sequence, the initiation data retrieved in step (c) (ii) is the same as the initiation data used in step (a) (i) and the retrieved code received in step (c) (iii) is the same as the identification code data used in step (a) (i) whereby the identification key produced in step (c) (iii) is the same as the identification key produced in step (a) (i).

12. Apparatus to be located at a service point for achieving secure cryptographic data communication, concerning a customer to be serviced, with a predetermined one of plural remote stations via a predetermined one of plural intermediate data processing nodes and wherein (1) each said remote station maintains addressable stored key data KD1" for each valid customer and stored key data KD2" for the remote station addressable via data representing each valid node; and (2) each said node maintains node identification data NID for transmission to the remote station, addressable stored key data KD3' representing each valid service point, and addressable stored key data KD2' representing each valid remote station, wherein KD3' is encrypted by KD2' and transmitted to the remote station where it is decrypted by KD2" to yield key data KD3" corresponding to the service point which is then combined with DK1" to generate a cryptographic transaction key at the remote station; said apparatus comprising at each service point:

data reader means for generating key data KD1 and further data D1 representing said customer and for also generating data D2 representing the remote station;

data storage means for storing key data KD3 and further data D3 representing the service point;

key generation means for combining said DK1 and KD3 data to produce a cryptographic transaction key at the service point identical to the one generated at the remote station; and

means for transmitting to said node said D1, D2 and D3 data.

13. Apparatus as in claim 12 further comprising at each node:

data storage means for storing said KD2' and KD3' data and for addressably accessing same using said D2 and D3 data respectively received from a service point;

data storage means storing said NID data;

encryption means for encrypting one of said accessed KD3' and KD2' data using the other as a key producing encrypted data KD2'(DK3'); and

means for transmitting to said remote station said D1, KD2'(DK3') and NID data.

14. Apparatus as in claim 13 further comprising at each remote station:

data storage means for storing said KD1" and KD2" data and for addressably accessing same using said D1 and NID data respectively received from a node;

decryption means for decrypting said KD2'(KD3') data using said accessed KD2" data as a key producing decryped data KD3"; and

key generation means for combining said KD1" and KD3" data to produce a cryptographic transaction key at the remote station identical to the one generated at the service point.

* * * * *

United States Patent [19]

Tanaka

[11] **Patent Number: 5,029,208**

[45] **Date of Patent: Jul. 2, 1991**

[54] **CIPHER-KEY DISTRIBUTION SYSTEM**

[75] Inventor: **Kazue Tanaka,** Tokyo, Japan

[73] Assignee: **NEC Corporation,** Tokyo, Japan

[21] Appl. No.: **488,952**

[22] Filed: **Mar. 5, 1990**

[30] **Foreign Application Priority Data**

Mar. 3, 1989	[JP]	Japan	1-52352
Mar. 3, 1989	[JP]	Japan	1-52353
Mar. 3, 1989	[JP]	Japan	1-52354
Mar. 30, 1989	[JP]	Japan	1-80501

[51] **Int. Cl.^{5}** **H04L 9/00**

[52] **U.S. Cl.** **380/21;** 380/30

[58] **Field of Search** 380/21, 30, 46

[56] **References Cited**

U.S. PATENT DOCUMENTS

Re. 33,189	3/1990	Lee et al.	380/21
4,200,700	4/1980	Mäder	521/186
4,228,321	10/1980	Flanagan	380/21
4,731,840	3/1988	Mniszewski et al.	380/21
4,876,716	10/1989	Okamoto	380/21
4,926,478	5/1990	Gruenberg	380/21
4,933,971	6/1990	Bestock et al.	380/21

OTHER PUBLICATIONS

Diffie, et al, "New Direction in Cryptography", IEEE Transaction on Information Theory, vol. 22, No. 6, p. 644, Nov. 1976.

Okamoto, "Key Distribution Systems Based on Identification Information", Advances in Cryptology—Crypto '87, pp. 196–202.

Okamoto, et al, "Identity-Based Information Security Management System for Personal Computer Networks", IEEE Journal on Selected Areas in Communications, vol. 7, No. 2, 1989.

Okamoto, et al, "Key Distribution System Based on Identification Information", IEEE/IEICE Global Telecommunications Conference 1987, Nov. 15–18, Tokyo, Japan.

Primary Examiner—Thomas H. Tarcza
Assistant Examiner—David Cain
Attorney, Agent, or Firm—Foley & Lardner

[57] **ABSTRACT**

A cipher-key distribution system used in a one-way communication from a first party to a second party. The cipher-key distribution system is composed of a first subsystem, a second subsystem, and a common file which stores information publically accessible by the first and second subsystems. The first subsystem generates a cipher-key based on a constant, receiving party identifying information, a random number, and public information from the common file. The first subsystem also generates a key distributing code based on a constant, a random number and a first secret information and transfers the key distributing code to a second subsystem. The second subsystem receives the key distributing code and information for identifying the first party and generates a second cipher-key identical to the cipher-key generated by the first subsystem. The second cipher-key is created from the information for identifying the first party, a second secret information, and the key distributing code. The first subsystem, instead of generating and transmitting a key distributing code, may simply transmit information for identifying the first communicating party to the second subsystem.

5 Claims, 11 Drawing Sheets

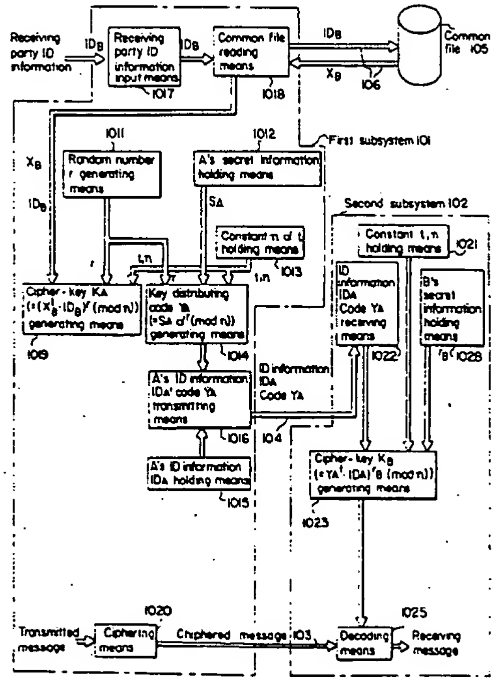
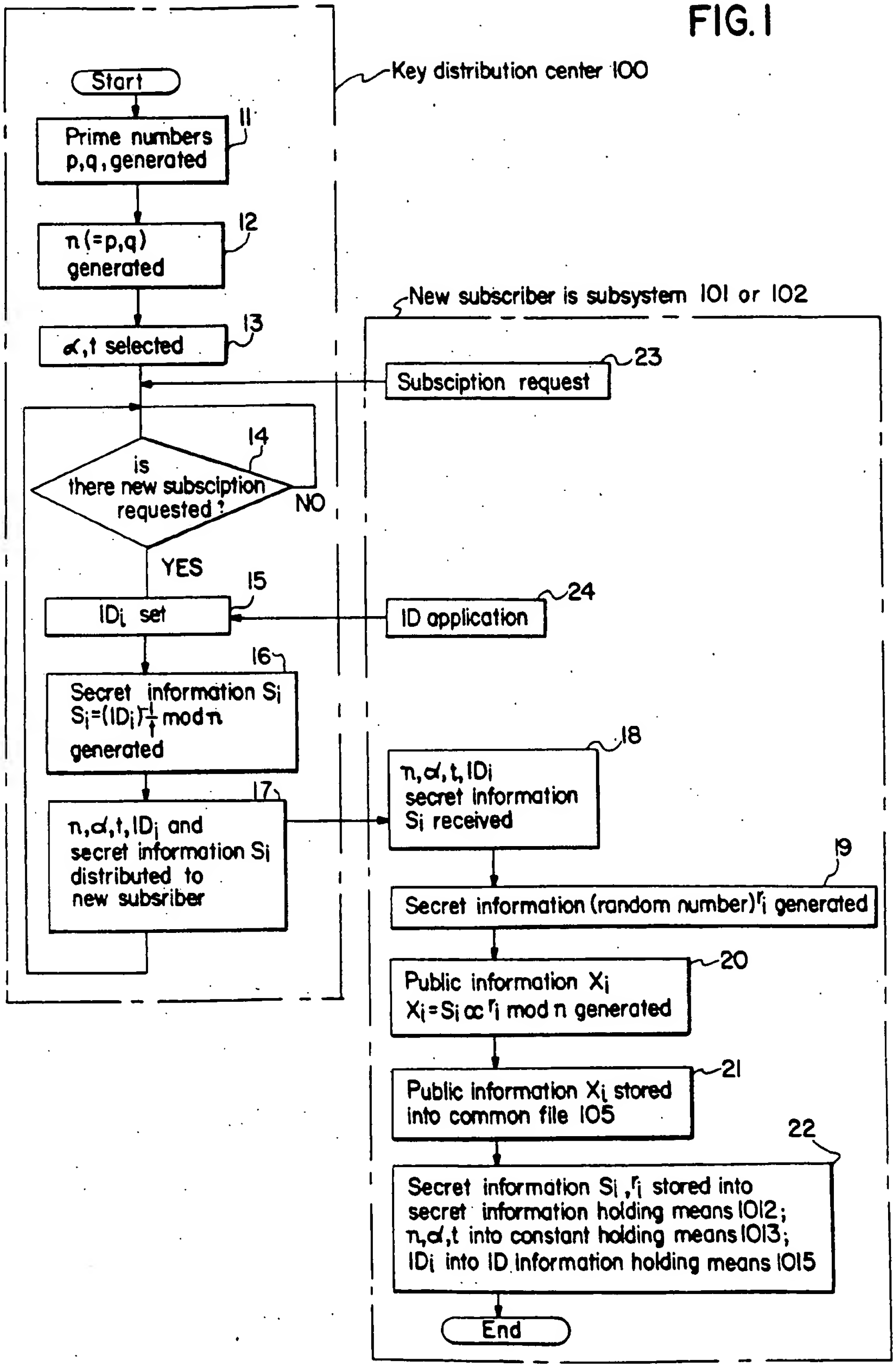

Receiving party ID information
ID_B
Receiving party ID information input means
1017
ID_B
Common file reading means
1018
ID_B
X_B
106
Common file 105
First subsystem 101
X_B
ID_B
1011
Random number r generating means
1012
A's secret information holding means
SA
Constant n of t holding means
1013
t,n
t,n
r
Cipher-key KA (=$(X_B^t \cdot ID_B)^r$ (mod n)) generating means
1019
Key distributing code YA (=SA α^r (mod n)) generating means
1014
A's ID information IDA' code YA transmitting means
1016
A's ID information IDA holding means
1015
ID information IDA Code YA
104
Second subsystem 102
Constant t, n holding means
1021
ID information IDA Code YA receiving means
1022
B's secret information holding means
r_B
1028
Cipher-key K_B (=$(YA^t \cdot IDA)^{r_B}$ (mod n)) generating means
1023
1020
Transmitted message
Ciphering means
Chiphered message 103
1025
Decoding means
Receiving message

FIG.1


Key distribution center 100
Start
Prime numbers p,q, generated
11
$n(=p,q)$ generated
12
α,t selected
13
is there new subsciption requested ?
14
NO
YES
ID_i set
15
Secret information S_i $S_i=(ID_i)^{-\frac{1}{t}} \bmod n$ generated
16
n,α,t,ID_i and secret information S_i distributed to new subsriber
17
New subscriber is subsystem 101 or 102
Subsciption request
23
ID application
24
n,α,t,ID_i secret information S_i received
18
Secret information (random number)r_i generated
19
Public information X_i $X_i=S_i\alpha^{r_i} \bmod n$ generated
20
Public information X_i stored into common file 105
21
Secret information S_i ,r_i stored into secret information holding means 1012; n,α,t into constant holding means 1013; ID_i into ID information holding means 1015
22
End

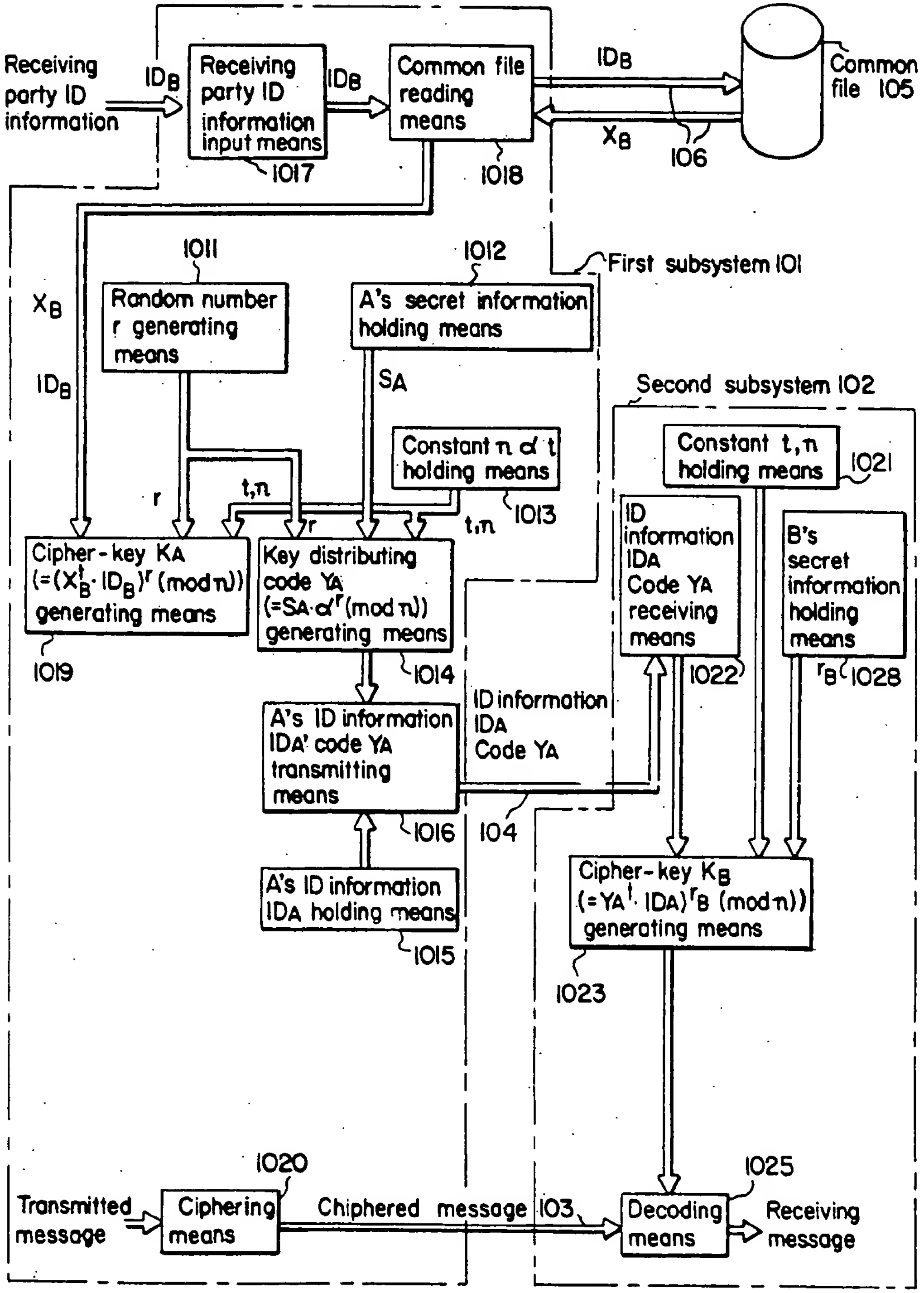

Receiving party ID information
ID_B
Receiving party ID information input means
ID_B
Common file reading means
ID_B
Common file 105
X_B
106
1017
1018
First subsystem 101
X_B
ID_B
1011
Random number r generating means
1012
A's secret information holding means
S_A
Constant n α t holding means
1013
t,n
r
t,n
r
Cipher-key K_A $(=(X_B^t \cdot ID_B)^r \pmod n)$ generating means
1019
Key distributing code Y_A $(=S_A \cdot \alpha^r \pmod n)$ generating means
1014
A's ID information ID_A' code Y_A transmitting means
1016
A's ID information ID_A holding means
1015
ID information ID_A Code Y_A
104
Second subsystem 102
Constant t,n holding means
1021
ID information ID_A Code Y_A receiving means
1022
B's secret information holding means
r_B
1028
Cipher-key K_B $(=Y_A{}^t \cdot ID_A)^{r_B} \pmod n))$ generating means
1023
1020
Transmitted message
Ciphering means
Chiphered message
103
Decoding means
1025
Receiving message

FIG. 2

FIG. 3

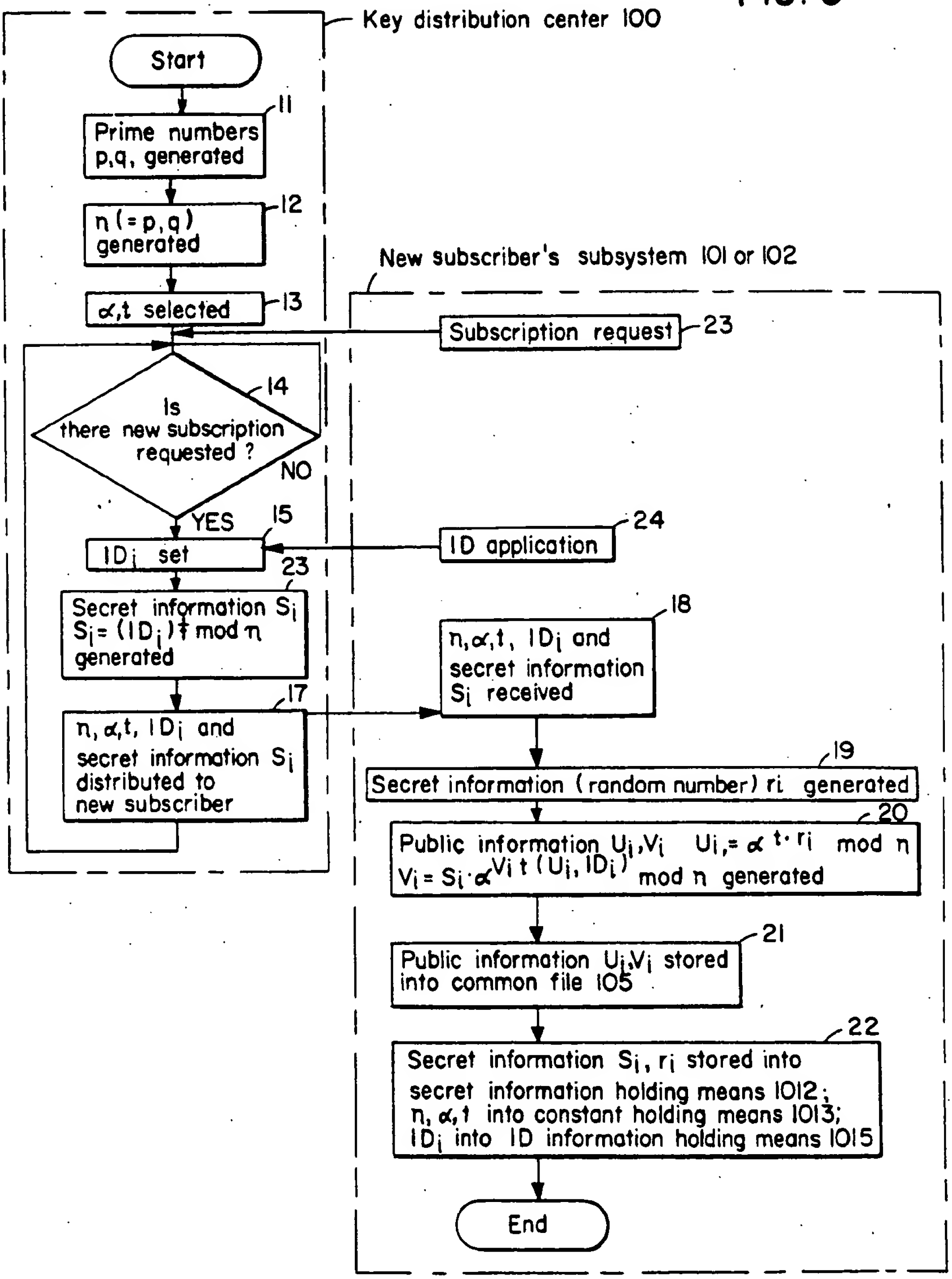
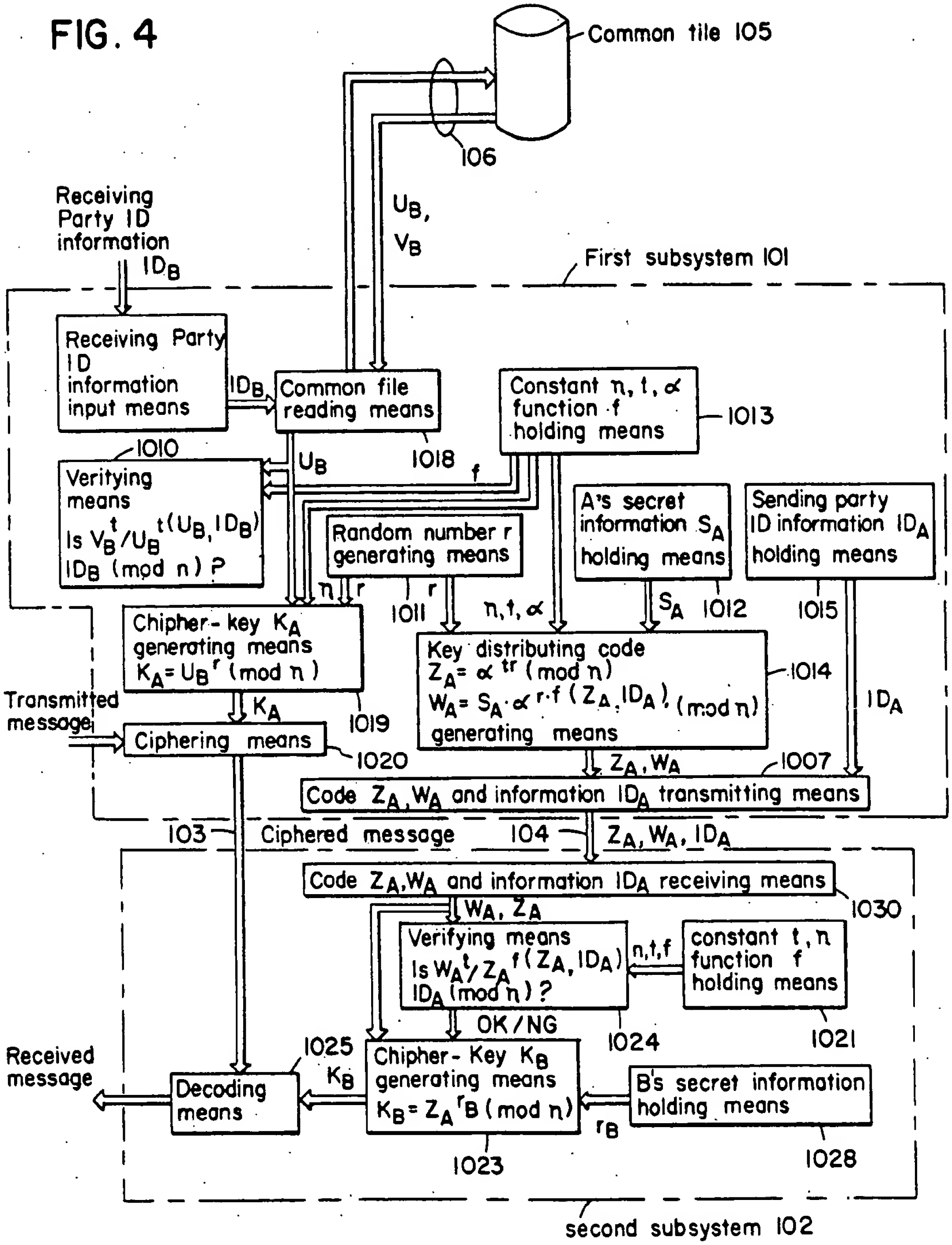

Key distribution center 100
Start
Prime numbers p,q, generated
11
n (=p,q) generated
12
α,t selected
13
Is there new subscription requested ?
14
NO
YES
IDi set
15
Secret information Si Si = (IDi)t mod n generated
23
n, α,t, IDi and secret information Si distributed to new subscriber
17
New subscriber's subsystem 101 or 102
Subscription request
23
ID application
24
n,α,t, IDi and secret information Si received
18
Secret information (random number) ri generated
19
Public information Ui,Vi Ui,= α t·ri mod n Vi = Si·α Vi t (Ui, IDi) mod n generated
20
Public information Ui,Vi stored into common file 105
21
Secret information Si, ri stored into secret information holding means 1012; n, α,t into constant holding means 1013; IDi into ID information holding means 1015
22
End

FIG. 4


Common tile 105
106
U_B, V_B
Receiving Party ID information
ID_B
First subsystem 101
Receiving Party ID information input means
ID_B
Common file reading means
1018
Constant n, t, α function f holding means
1013
1010
Veritying means Is $V_B^t/U_B^{t(U_B, ID_B)}$ ID_B (mod n) ?
U_B
f
Random number r generating means
1011
r
n
r
A's secret information S_A holding means
S_A
1012
Sending party ID information ID_A holding means
1015
ID_A
n, t, α
Chipher-key K_A generating means $K_A = U_B^r$ (mod n)
1019
K_A
Key distributing code $Z_A = \alpha^{tr}$ (mod n) $W_A = S_A \cdot \alpha^{r \cdot f(Z_A, ID_A)}$ (mod n) generating means
1014
Transmitted message
Ciphering means
1020
Z_A, W_A
1007
Code Z_A, W_A and information ID_A transmitting means
103
Ciphered message
104
Z_A, W_A, ID_A
Code Z_A, W_A and information ID_A receiving means
1030
W_A, Z_A
Verifying means Is $W_A^t/Z_A^{f(Z_A, ID_A)}$ ID_A (mod n) ?
n,t,f
constant t, n function f holding means
1024
1021
OK / NG
Received message
Decoding means
1025
K_B
Chipher-Key K_B generating means $K_B = Z_A^{r_B}$ (mod n)
r_B
B's secret information holding means
1023
1028
second subsystem 102

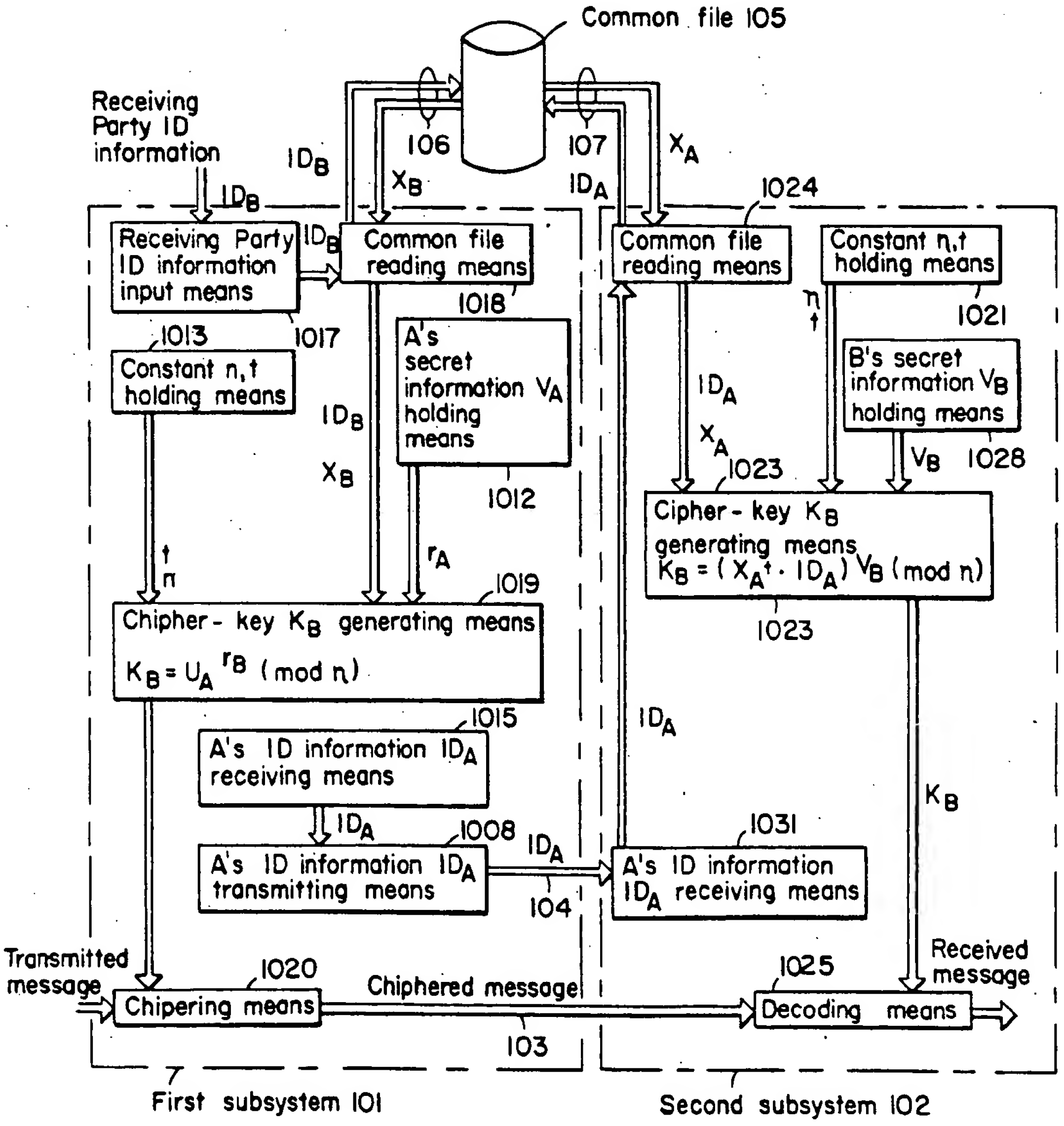

Common file 105
Receiving Party ID information
ID_B
106
107
X_B
ID_A
X_A
1024
Receiving Party ID information input means
Common file reading means
1018
1017
1013
Constant n, t holding means
A's secret information V_A holding means
ID_B
X_B
1012
t
n
r_A
1019
Chipher- key K_B generating means
$K_B = U_A^{r_B}$ (mod n)
1015
A's ID information ID_A receiving means
1008
A's ID information ID_A transmitting means
104
Transmitted message
1020
Chipering means
Chiphered message
103
First subsystem 101
Common file reading means
Constant n, t holding means
1021
B's secret information V_B holding means
V_B
1028
1023
Cipher- key K_B generating means
$K_B = (X_A^t \cdot ID_A)^{V_B}$ (mod n)
1023
K_B
1031
A's ID information ID_A receiving means
1025
Decoding means
Received message
Second subsystem 102

FIG. 5

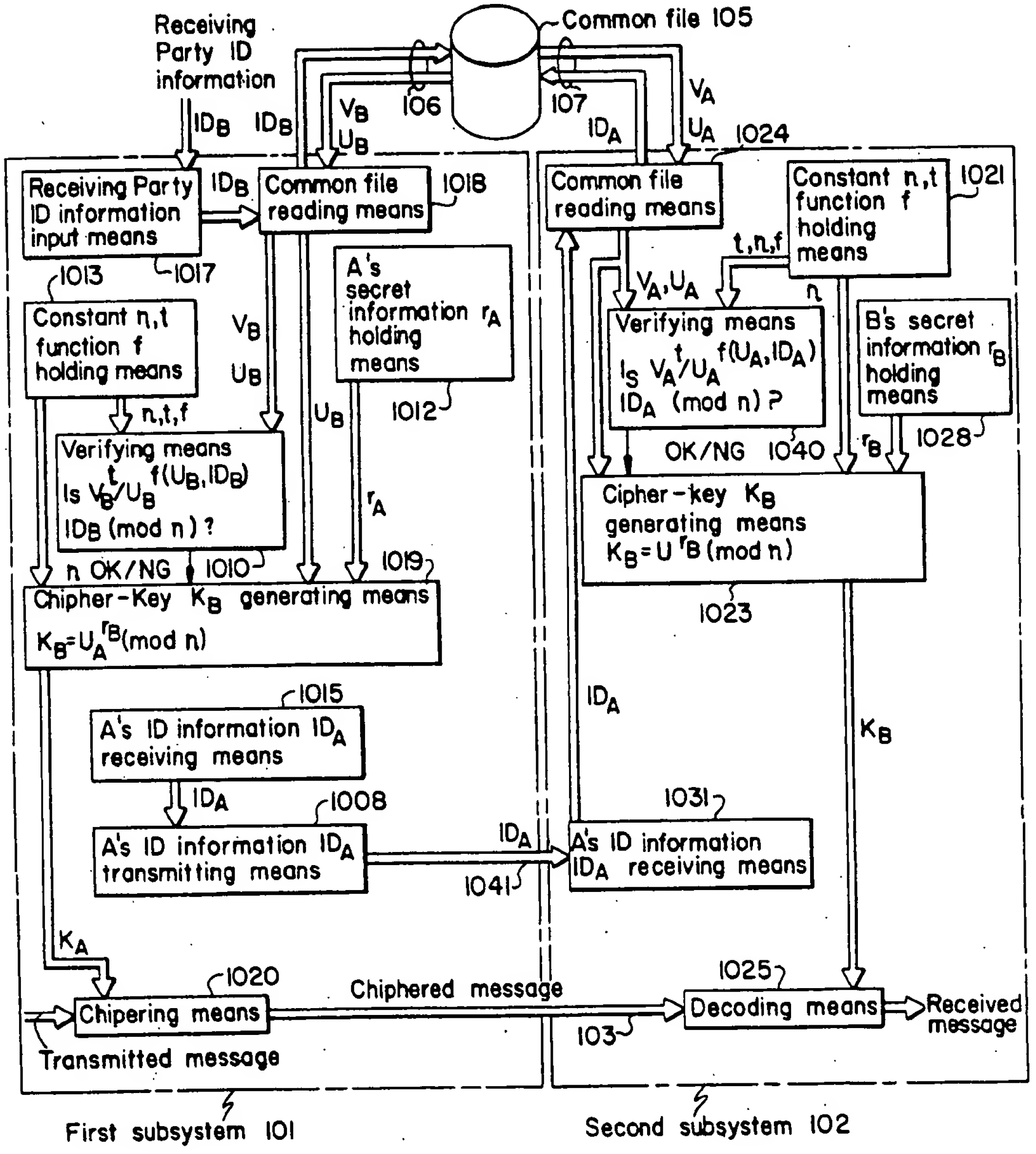

Receiving Party ID information
Common file 105
ID_B
ID_B
V_B
U_B
106
107
ID_A
V_A
U_A
1024
Receiving Party ID information input means
1017
ID_B
Common file reading means
1018
Common file reading means
Constant n,t function f holding means
1021
1013
Constant n,t function f holding means
V_B
U_B
A's secret information r_A holding means
1012
U_B
n,t,f
Verifying means Is $V_B^t/U_B^{f(U_B,ID_B)}$ ID_B (mod n) ?
r_A
n OK/NG
1010
1019
Chipher-Key K_B generating means $K_B=U_A^{r_B}$(mod n)
t,n,f
V_A,U_A
n
Verifying means Is $V_A^t/U_A^{f(U_A,ID_A)}$ ID_A (mod n) ?
B's secret information r_B holding means
OK/NG
1040
r_B
1028
Cipher-key K_B generating means $K_B=U^{r_B}$(mod n)
1023
1015
A's ID information ID_A receiving means
ID_A
1008
A's ID information ID_A transmitting means
ID_A
1041
ID_A
1031
A's ID information ID_A receiving means
K_B
K_A
1020
Chipering means
Transmitted message
Chiphered message
103
1025
Decoding means
Received message
First subsystem 101
Second subsystem 102

FIG.6

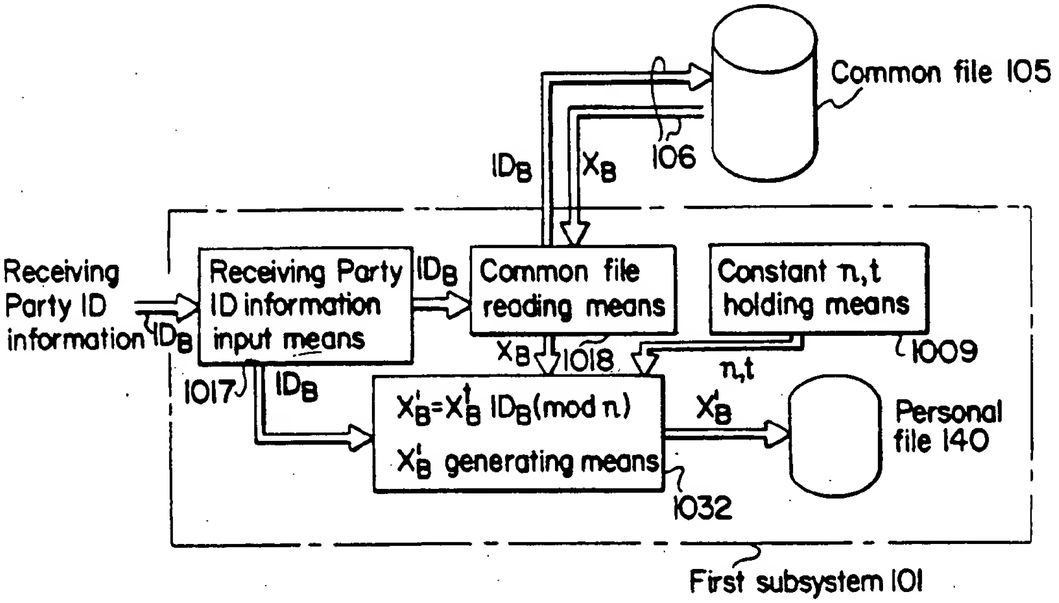

Common file 105
106
ID_B
X_B
Receiving Party ID information
ID_B
Receiving Party ID information input means
ID_B
Common file reading means
Constant n,t holding means
1009
X_B
1018
n,t
1017
ID_B
$X'_B=X^t_B\ ID_B(\bmod n)$
X'_B generating means
X'_B
Personal file 140
1032
First subsystem 101

FIG. 7

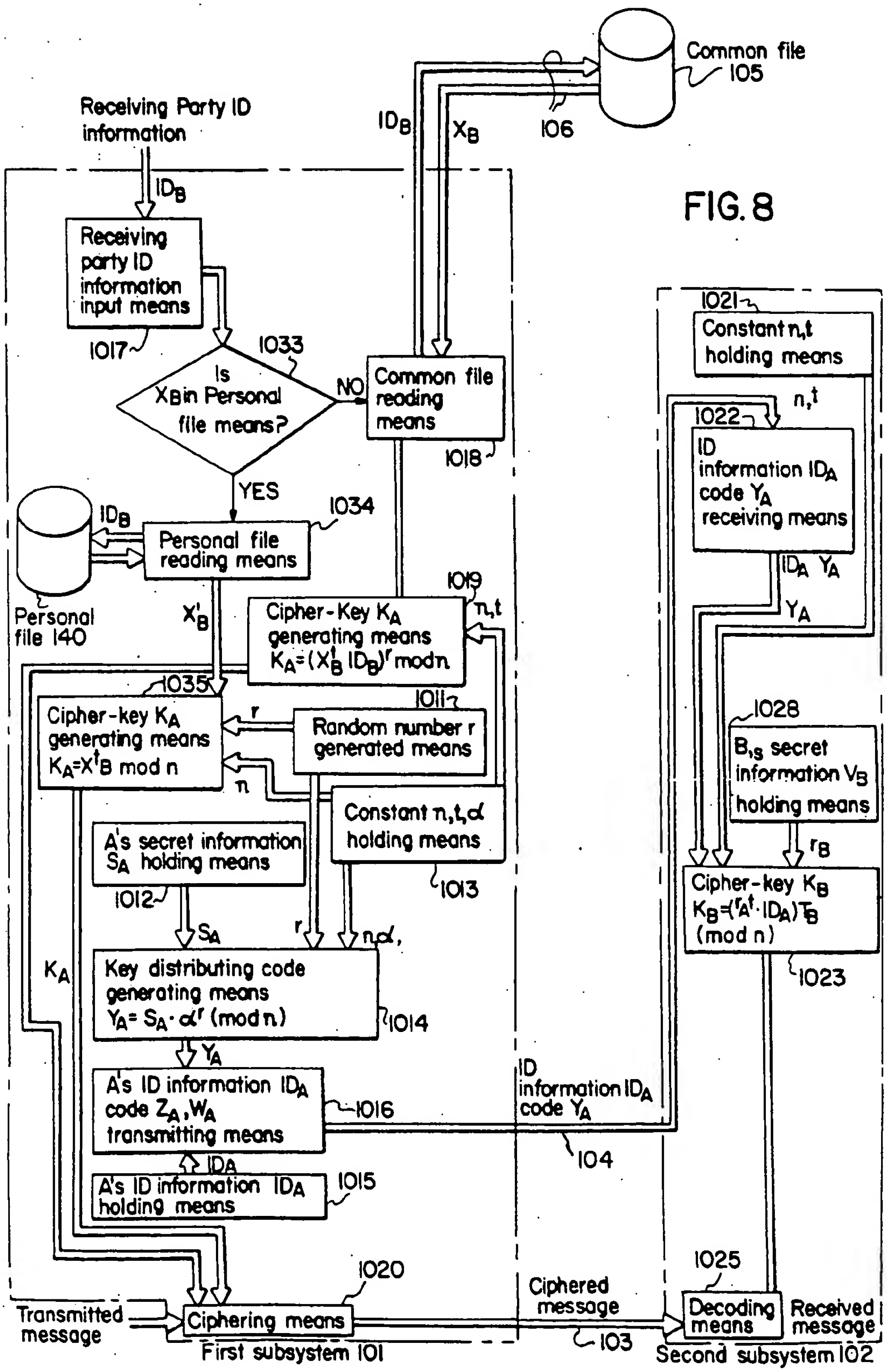

Common file
105
106
IDB
XB
Receiving Party ID information
IDB
Receiving party ID information input means
1017
1033
Is XB in Personal file means?
NO
Common file reading means
1018
YES
1034
IDB
Personal file reading means
Personal file 140
X'B
1019
Cipher-Key KA generating means KA=(X'tB IDB)r mod n
n,t
1035
Cipher-key KA generating means KA=X'tB mod n
r
Random number r generated means
1011
n
Constant n,t,α holding means
1013
A's secret information SA holding means
1012
SA
r
n,α,
KA
Key distributing code generating means YA=SA·αr (mod n)
1014
YA
A's ID information IDA code ZA,WA transmitting means
1016
IDA
A's ID information IDA holding means
1015
ID information IDA code YA
104
1020
Transmitted message
Ciphering means
First subsystem 101
Ciphered message
103
1021
Constant n,t holding means
n,t
1022
ID information IDA code YA receiving means
IDA YA
YA
1028
B,s secret information VB holding means
rB
Cipher-key KB KB=(rAt·IDA)rB (mod n)
1023
1025
Decoding means
Received message
Second subsystem 102

FIG. 8

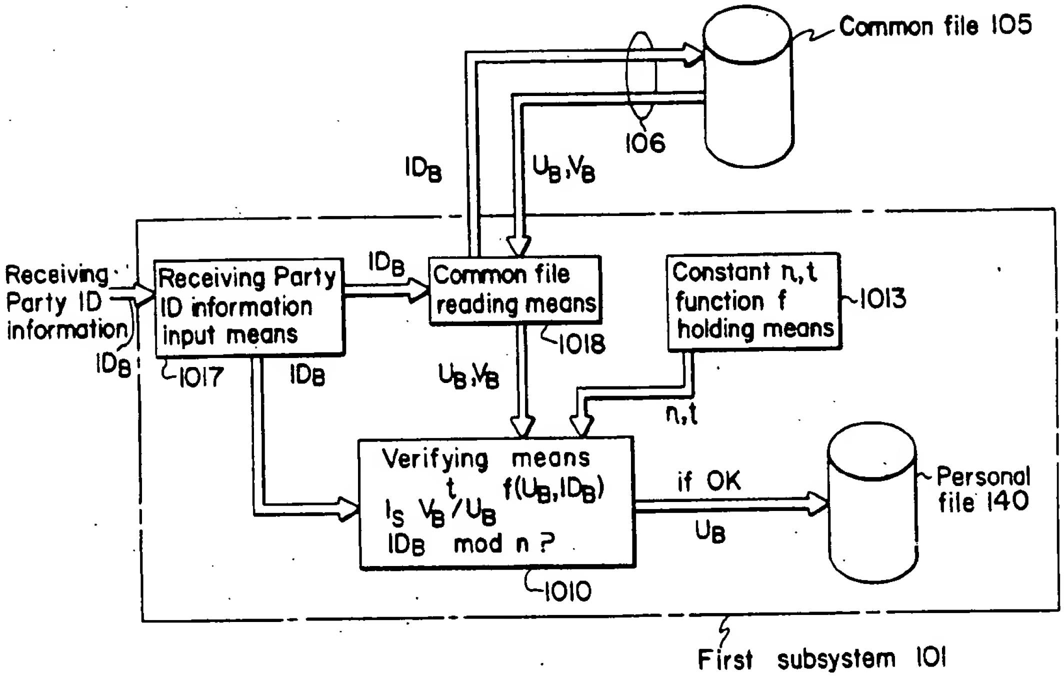

Common file 105
106
ID_B
U_B, V_B
Receiving Party ID information
ID_B
Receiving Party ID information input means
1017
ID_B
Common file reading means
1018
U_B, V_B
Constant n, t function f holding means
1013
n, t
Verifying means
Is $V_B^t / U_B^{f(U_B, ID_B)}$ ID_B mod n ?
1010
if OK
U_B
Personal file 140
First subsystem 101

FIG.9

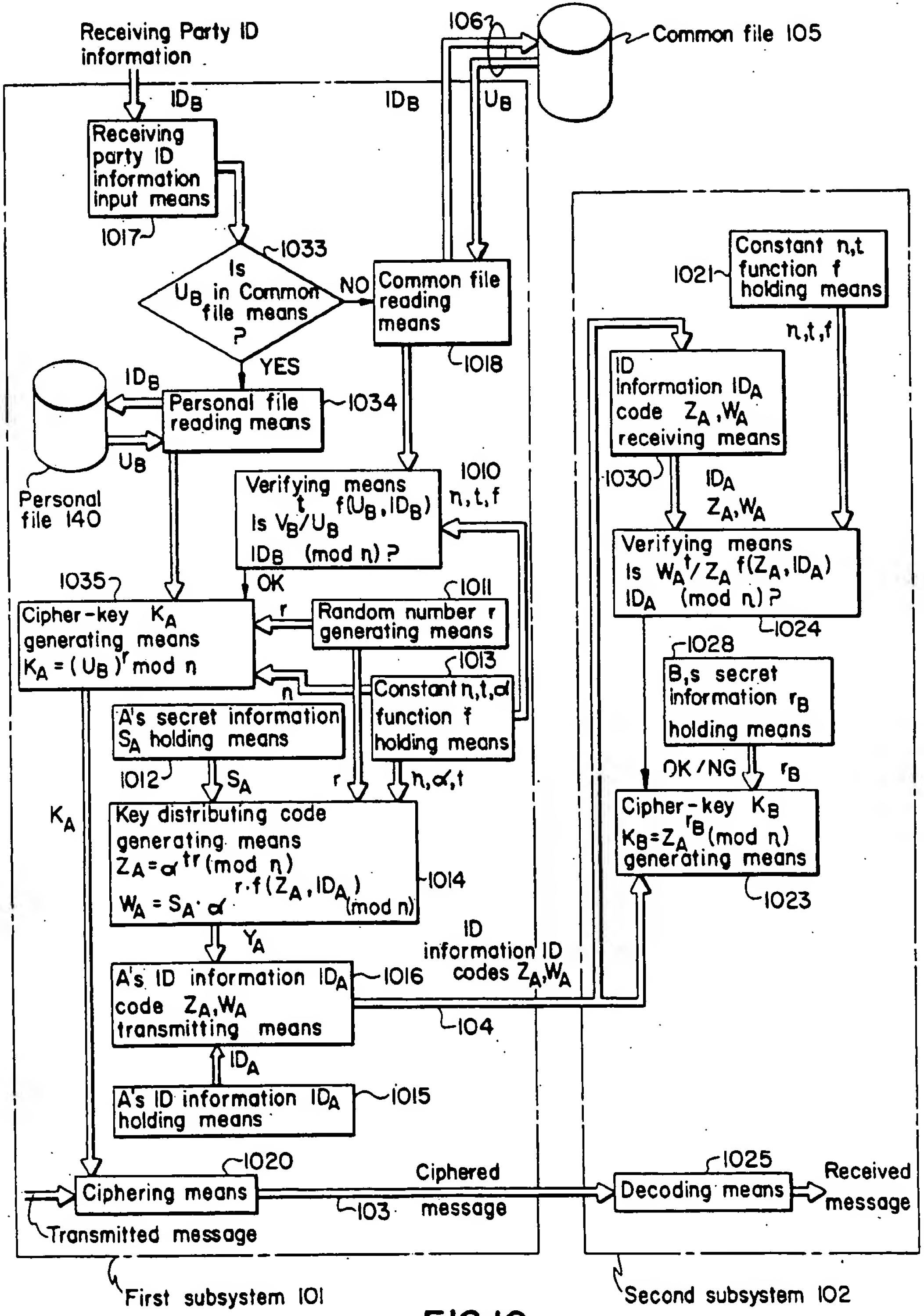

Receiving Party ID information
ID_B
106
Common file 105
ID_B
U_B
Receiving party ID information input means
1017
1033
Is U_B in Common file means ?
NO
YES
Common file reading means
1018
ID_B
Personal file reading means
1034
U_B
Personal file 140
Verifying means
Is $V_B^t/U_B^{f(U_B, ID_B)}$ ID_B (mod n) ?
1010
n, t, f
OK
1035
Cipher-key K_A generating means
$K_A = (U_B)^r \bmod n$
r
Random number r generating means
1011
n
1013
Constant n,t,α function f holding means
A's secret information S_A holding means
1012
S_A
r
n,α,t
K_A
Key distributing code generating means
$Z_A = \alpha^{tr} \pmod n$
$W_A = S_A \cdot \alpha^{r \cdot f(Z_A, ID_A)} \pmod n$
1014
Y_A
A's ID information ID_A code Z_A, W_A transmitting means
1016
ID information ID codes Z_A, W_A
104
ID_A
A's ID information ID_A holding means
1015
1020
Ciphering means
Transmitted message
Ciphered message
103
First subsystem 101
Constant n,t function f holding means
1021
n,t,f
ID information ID_A code Z_A, W_A receiving means
1030
ID_A
Z_A, W_A
Verifying means
Is $W_A^t/Z_A^{f(Z_A, ID_A)}$ ID_A (mod n) ?
1024
1028
B,s secret information r_B holding means
OK/NG
r_B
Cipher-key K_B
$K_B = Z_A^{r_B} \pmod n$
generating means
1023
1025
Decoding means
Received message
Second subsystem 102

FIG.10

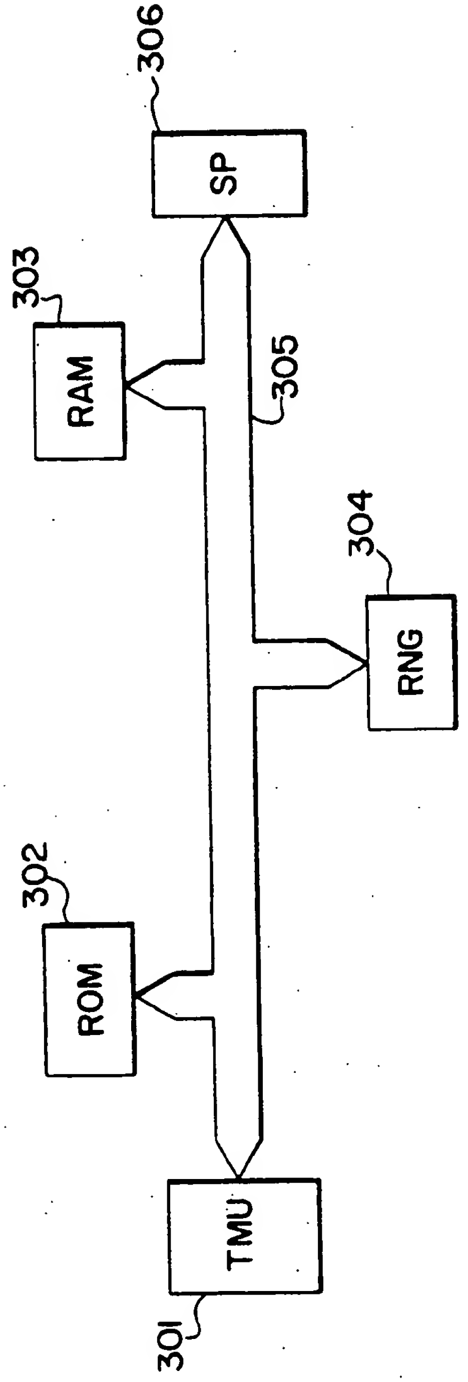


FIG. 11

CIPHER-KEY DISTRIBUTION SYSTEM

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to a key distribution system for the one-way communication, from a sending party to a receiving party, of a cipher-key for use in conventional cryptosystems.

BACKGROUND OF THE INVENTION

Well-known prior art key distribution systems include the Diffie-Hellman (DH) system and the ID-based system. The former is disclosed in Diffie and Hellman, "New Direction in Cryptography" in the IEEE Transaction on Information Theory, Vol. 22, No. 6, p. 644. According to the DH system which stores public information for each communicating party, if party A is to communicate with party B in cipher, A prepares a cipher-key from B's public information Y_B and its own secret information X_A. This method, however, allows another party to pretend to be an authorized party by illegitimately altering public information.

For information on the latter, the ID-based key distribution system, reference may be made to the U.S. Pat. No. 4,876,716, uses public identification information such as the name of each communicating party to prepare a cipher-key. The ID-based system is immune from illegitimate alteration of public information. As it requires two-way communication, however, there is the problem of imposing large overhead on both the sending and the receiving parties if a cryptogram is to be sent by an existing mail system.

The DH key distribution system also involves the problem of letting an unauthorized receiver pretend to be an authorized user by altering public information.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a system cleared of the above mentioned disadvantages.

A first system according to one aspect of the invention is a cipher-key distribution system for distributing a cipher key for use in cipher communication by one party with another, provided with:

a common file for storing public information in a position indicated by receiving party identifying information, and first and second subsystems, wherein:

said first subsystem comprises:

reading means for reading said public information out of said common file;

random number generating means for generating random numbers;

first cipher-key generating means for generating a cipher key on the basis of a constant, said receiving party identifying information given from outside, a random number generated by said random number generating means and the public information read out by said reading means;

secret information holding means for holding the secret information of the communicating party using this subsystem;

key distributing code generating means for generating a key distributing code on the basis of said constant, said random number and the secret information given from said secret information holding means; and

transmitting means for transmitting the key distributing code generated by the key distributing code generating means and the information for identifying the communicating party, and

said second subsystem comprises:

receiving means for receiving the key distributing code and the identifying information from said transmitting means of the first subsystem;

constant holding means for holding the constant;

secret information holding means for holding the secret information of the communicating party using this subsystem; and

second cipher-key generating means for generating a cipher key, which is identical with the cipher-key generated by said first cipher-key generating means, on the basis of the key distributing code and identifying information from said receiving means, the constant from said constant holding means and the secret information from said secret information holding means.

A second system according to another aspect of the invention is a cipher-key distribution system for distributing a cipher key for use in cipher communication by one party with another, provided with:

a common file for storing public information in a position indicated by receiving party identifying information, and first and second subsystems, wherein:

said first subsystem comprises:

first reading means for reading said public information out of said common file;

secret information holding means for holding the secret information of the communicating party using this subsystem;

first cipher-key generating means for generating a cipher key on the basis of a constant, receiving party identifying information given from outside, the public information read out by said first reading means and the secret information from said secret information holding means; and

transmitting means for transmitting the information for identifying the communicating party using this subsystem, and

said second subsystem comprises:

receiving means for receiving the identifying information given from said transmitting means;

constant holding means for holding the constant;

secret information holding means for holding the secret information of the communicating party using this subsystem;

second reading means for reading said public information out of said common file, and

second cipher-key generating means for generating a cipher key, which is identical with the cipher-key generated by said first cipher-key generating means, on the basis of the identifying information from said receiving means, the constant from said constant holding means, the secret information from said secret information holding means, and the public information given from said second reading means.

A third system according to still another aspect of the invention has, within the first subsystem of the first system, a personal file for storing part of the information stored in the common file.

A fourth system according to yet another aspect of the invention has, within the first subsystem or subsystems of at least one of the first, second and third systems, verifying means for verifying the information read out of the common file.

BRIEF DESCRIPTION OF THE DRAWINGS

Other features and advantages of the present invention will become more apparent from the following detailed description when taken in conjunction with the accompanying drawings in which:

FIG. 1 shows preparatory steps for first, third and fifth preferred embodiments of the invention;

FIG. 2 illustrates the first preferred embodiment of the invention;

FIG. 3 shows preparatory steps for second, fourth and sixth preferred embodiments of the invention;

FIG. 4 illustrates the second preferred embodiment of the invention;

FIG. 5 illustrates the third preferred embodiment of the invention;

FIG. 6 illustrates the fourth preferred embodiment of the invention;

FIG. 7 illustrates the preparation for the fifth preferred embodiment of the invention, taking place after the preparatory steps shown in FIG. 1;

FIG. 8 illustrates the fifth preferred embodiment of the invention;

FIG. 9 illustrates the preparation for the sixth preferred embodiment of the invention, taking place after the preparatory steps shown in FIG. 3;

FIG. 10 illustrates the sixth preferred embodiment of the invention; and

FIG. 11 illustrates the configurations of the first subsystem 101 and the second subsystem 102 shown in FIGS. 2 and 4 through 10.

In the figures, the same reference numerals denote respectively the same constituent elements.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to FIGS. 2, 4, 8 and 10, each of the preferred embodiments of the present invention illustrated therein includes a first subsystem 101, a second subsystem 102, an insecure cryptogram communication channel 103 for transmitting a cryptogram from the subsystem 101 to the subsystem 102, an insecure intermediate key communication channel 104 for transmitting a code Y_A for distributing a coded key from the subsystem 101 to the subsystem 102, a common file 105 for storing public information X_i containing identifying information ID_i, and a line 106 for connecting the common file 105 and the subsystem 101. The subsystems 101 and 102 are used by communicating parties A and B, respectively.

First will be described in detail the procedure of registration into the common file 105, which is one of the characteristic features of the present invention, with reference to FIGS. 1 through 3.

This action takes place before a cryptogram is transmitted.

FIG. 1 shows how preparations are made for the generation of cipher-keys K_A and K_B in a preferred embodiment of the invention.

First, large prime numbers p and q are selected (step 11). Then the product n of these two large prime numbers p and q is calculated (step 12). Further, t is selected as a number mutually prime to $(p-1)\cdot(q-1)$, and α is selected as a positive integer smaller than n, which becomes a primitive element GF(p) and GF(q) (step 13). After that, either the subsystem 101 or 102 on the part of a new subscriber gives a subscription request 23 as required. At a key distribution center 100, an inquiry is made as to the presence or absence of a subscription request, and the inquiry is continued until a subscription request is given (step 14). When the inquiry at step 14 finds an affirmative reply, identifying information ID_i for the pertinent subscriber i is set in response to an ID application 24 by the subsystem 101 or 102 (step 15). Next, by using this identifying information ID_i, secret information S_i is figured out by the following equation (step 16):

$$S_i=(ID_i)^{-1/t} \bmod n$$

where a(mod b) means the remainder of the division of a by b. To the new subscriber i are distributed n, α, t, ID_i and S_i, generated at these steps 12, 13 and 16 (step 17).

The system on the part of the new subscriber i receives n, α, t, ID_i and the secret information S_i distributed at step 17 (step 18). Next, another piece of secret information (a random number) r_i is generated (step 19). Then, on the basis of the received secret information S_i, the newly generated information r_i and α, which became a primitive element at step 13, public information X_i is generated by the following equation (step 20):

$$X_i=S_i\cdot\alpha^{r_i} \bmod n$$

Referring to FIGS. 1 and 3, the generated public information X_i is stored into a designated address ID_i in the common file 105. Then the secret information pieces S_i and r_i are stored into secret information holding means 1012, n, α and t are stored into constant holding means 1013 and, at the same time, ID_i is stored into identifying information holding means 1015 (step 22). Steps 11 to 17 are assigned to the key distribution center 100. The identifying information ID_i, which is assigned by the center to be different from one communicating party to another, turns generally known pieces of information such as the personal name and address into identifying codes according to, for instance, the ASCII formula.

Now will be described in detail, with reference to FIG. 2, a first preferred embodiment of the present invention in which the public information stored in the common file 105 is accessed by each communicating party.

It is supposed that, in this first preferred embodiment, a sending party A accesses the common file 105, and that, at the key distribution center 100, a conversion formula and a common parameter are set and personal secret information is distributed as shown in FIG. 1. The subsystem 101 generates a random number from random number generating means 1011 and, at the same time, reads out secret information S_A from the secret information holding means 1012 for A and constants d and n from the constant holding means 1013. Then key distribution code Y_A generating means 1014 generates a code Y_A as an intermediate cipher-key in accordance with:

$$Y_A=S_A\cdot\alpha^r (\bmod n)$$

The code Y_A generated by the generating means 1014 and identifying information ID_A for A are sent out to the line 104 by transmitting means 1016. Code Y_A receiving means 1022 of the subsystem 102 receives the code Y_A provided via the line **104** and the identifying information ID_A. Using the identifying information ID_A and the code Y_A from the receiving means **1022**, constants t and n from constant holding means **1021**, and secret information r_B from secret information holding means **1028** for B, cipher-key K_B generating means **1023** generates a cipher-key K_B in accordance with:

$$K_B=(Y_A^t\cdot ID_A)^{r_B}(\mathrm{mod}\ n)$$

Here $K_B=\alpha^{r_B t\ r}(\mathrm{mod}\ n)$ because $Y_A=S_A^t\cdot\alpha^{r_A t}$

$=(ID_A)^{-1}\cdot\alpha^{r_A t}(\mathrm{mod}\ n)$.

There is no need to send second key distributing information from the second subsystem **102** to the subsystem **101** of the sending party A, because public information on the receiving party B is stored in the common file **105** and therefore the subsystem **101** for itself can read out this public information.

Thus the subsystem **101** obtains identifying information ID_B for the receiving party B from outside with input means **1017** and, at the same time, common file reading means **1018** uses this information ID_B to read out public information X_B on B from the common file **105**.

Cipher-key generating means **1019**, using these pieces of information ID_B and X_B, generates a cipher-key K_A in accordance with:

$$K_A=(X_B^t\cdot ID_B)^r\mathrm{mod}\ n$$

Here $K_A=\alpha^{r_B\cdot t\cdot r}$ mod n because $X_B^t=S_B^t\cdot\alpha^{r_B t}$

$=(ID_B)^{-1}\cdot\alpha^{r_B t}$ (mod n).

Therefore, the cipher-key K_A generated by the cipher-key K_A generating means **1019** of the subsystem **101** and the cipher-key K_B generated by the cipher-key K_B generating means **1023** of the subsystem **102** become identical, so that key distribution can be achieved.

Thus the sending party A can cipher his message with the subsystem **101** by accessing the common file **105** with the identifying information ID_B for the receiving party B. The key can be generated irrespective of the presence or absence of the receiving party B, and the key distributing code Y_A and the identifying information ID_A can be transmitted together with the ciphered message.

An impostor intending to pretend to be a legitimate communicating party i by altering public information X_i can do so if he finds X and r to satisfy the following equation:

$$X^t\cdot ID_i=\alpha^{tr}\mathrm{mod}\ n$$

The difficulty to meet this requirement, however, even in collusion with another legitimate party is evident from, for instance, Advances in Cryptology—Crypto '87, pp. 196–202. This literature further explains that, even if said X_i is made public, neither S_i nor r_i, both secret information, can be disclosed.

Next will be described in detail, with reference to FIG. **4**, a second preferred embodiment of the invention, which is characterized by a procedure to verify public information after it is read out. .

First, preparatory steps for the execution of this second embodiment will be explained in detail with reference to FIG. 3.

Referring to FIG. **3**, first of all, large prime numbers p and q are selected (step **11**). Next, the product n of these two large prime numbers p and q is calculated (step **12**). Then, t is selected as a number mutually prime to $(p-1)\cdot(q-1)$; α is selected as a positive integer smaller than n, which becomes a primitive element in GF(p) and GF(q), and further is selected a two-variable one-way function f (step **13**). After that, either the subsystem **101** or **102** on the part of a new subscriber gives a subscription request **23** as required.

At a key distribution center **100**, an inquiry is made as to the presence or absence of a subscription request, and the inquiry is continued until a subscription request is given (step **14**). When the inquiry at step **14** finds an affirmative reply, identifying information ID_i for the pertinent subscriber i is set in response to an ID application **24** by the subsystem **101** or **102** (step **15**).

Next, by using this identifying information ID_i, secret information S_i is figured out by the following equation (step **16**):

$$S_i=(ID_i)^{1/t}\ \mathrm{mod}\ n$$

To the new subscriber i are distributed f, n, α, t, ID_i and S_i, generated at these steps **12**, **13** and **16** (step **17**).

The system on the part of the new subscriber i receives f, n, α, t, ID_i and the secret information S_i distributed at step **17** (step **18**). Next, a randon number r_i is generated (step **19**). Then, on the basis of the received secret information S_i, the newly generated secret information (random number) r_i and α, which became a primitive element at step **13**, pieces of public information U_i and V_i are generated by the following equation (step **20**):

$$U_i=\alpha^{t\cdot r_i}\ \mathrm{mod}\ n$$

$$V_i=S_i\cdot\alpha^{f(U_i, ID_i)\cdot r_i}\mathrm{mod}\ n$$

Referring to FIGS. **1** and **3**, the generated public information pieces U_i and V_i are stored into the common file **105**. Then the received secret information pieces S_i is stored into secret information holding means **1012**, n, α and t are stored into constant holding means **1013** and, at the same time, ID_i is stored into identifying information holding means **1015** (step **22**).

Steps **11** to **15** and **23** to **24** are assigned to the key distribution center **100**.

Now will be described in detail, with reference to FIG. **4**, a second preferred embodiment of the present invention in which the public information stored in the common file **105** is accessed by each communicating party.

It is supposed that, in this second preferred embodiment, a sending party A accesses the common file **105**, and that, at the key distribution center **100**, a conversion formula and a common parameter are set and personal secret information is distributed as shown in FIG. 3. The subsystem **101** generates a random number from random number generating means **1011** and, at the same time, reads out secret information S_A from the secret information holding means **1012** for A and constants n, t and α from the constant holding means **1013**. Then key distribution code Z_A and W_A generating means **1014** generates codes Z_A and W_A as intermediate cipher-keys in accordance with:

$$Z_A=\alpha^{tr}(\mathrm{mod}\ n)$$

$$W_A = S_A \cdot \alpha^{tf(Z_A,\, ID_A)} \pmod n$$

The codes Z_A and W_A generated by the generating means **1014** and identifying information ID_A for A are sent out to the line **104** by transmitting means **1007**. Receiving means **1030** of the subsystem **102** receives the codes Z_A and W_A provided via the line **104** and the identifying information ID_A. Using the identifying information ID_A and the codes Z_A and W_A from the receiving means **1030**, a function f from constant holding means **1021** and the constants t and n, verifying means **1024** checks whether or not $W_A^t/Z_A^{f(Z_A,\, ID_A)}$ is equal to ID_A(mod n).

If the verifying means **1024** verifies the equality, it sends an OK signal to generating means **1023**.

In response to this OK signal, the cipher-key generating means **1023**, using secret information r_B from holding means **1028**, generates a cipher-key K_B in accordance with:

$$K_B = Z_A^{r_B} \pmod n$$

Here, $K_B = \alpha^{t\,r\,r_B} \pmod n$.

There is no need to send second key distributing information from the second subsystem **102** to the subsystem **101** of the sending party A, because public information on the receiving party B is stored in the common file **105** and therefore the subsystem **101** for itself can read out this public information.

Thus the subsystem **101** obtains identifying information ID_B for the receiving party B from outside with input means **1017** and, at the same time, reading means **1018** reads out public information X_B on B from the common file **105** in accordance with this information ID_B(mod n).

Then, verifying means **1010** checks whether or not $W_B^t/U_B^{f(U_B,\, ID_B)}$ is equal to ID_B(mod n).

If the verifying means **1010** verifies the equality, it sends an OK signal to generating means **1019**.

The cipher-key generating means **1019**, using the public information U_B provided from reading means **1018**, generates a cipher-key K_A in accordance with:

$$K_A = U_B^t \pmod n$$

Here, $K_A = \alpha^{t\,r\,r_B} \pmod n$ because $U_B = \alpha^{r r_B} \bmod n$.

Thus is achieved key distribution as the cipher-key K_A generated by the cipher-key K_A generating means **1019** of the subsystem **101** and the cipher-key K_B generated by the cipher-key K_B generating means **1023** of the subsystem **102** become identical.

An impostor intending to pretend to be a legitimate communicating party i by altering public information U_i, V_i or key generating information Z_i, W_i can do so if he finds X and Y to satisfy the following equation:

$$X^{f(X,\, ID_i)} ID_i = Y^t \bmod n$$

The difficulty to meet this requirement, however, ever in collusion with another legitimate party is described in, for instance, IEEE Journal on Selected Areas in Communication, Vol. 7, No. 2, pp. 290–294. This literature further explains that, even if said U_i, V_i is made public or said Z_i, W_i is tapped. neither s_i, r_i nor r can be disclosed.

Next will be described in detail, with reference to FIG. 5, a third preferred embodiment of the invention, in which both the first subsystem **101** and the second subsystem access the common file **105**.

It is supposed that, in this third preferred embodiment, a sending party A and a receiving party B access the common file **105**, and that, at the key distribution center **100**, a conversion formula and a common parameter are set as shown in FIG. 1. Referring to FIG. 5, identifying information for the receiving party B is entered from input means **1017**. In response to this input, common file reading means **1018** reads out public information X_B on B from a position indicated by ID_B in the common file **105**. Cipher-key generating means **1019**, using secret information r_A from secret information holding means **1012** for A and constants n and t from constant holding means **1013**, generates a cipher key K_A in accordance with:

$$K_A = (X_B^t \cdot ID_B)^{r_A} \bmod n$$

Here, $K_A = \alpha^{r_B t\, r_A} \bmod n$ because $X_B^t = S_B^{S} \cdot \alpha^{r_B t} = (ID_B)^{-1 \cdot \alpha} r_B \pmod n$.

Identifying information ID_A from identifying information ID_A holding means **1015** for A is supplied to receiving means **1031** of the subsystem **102** via transmitting means **1008** and a line **104**. The information ID_A supplied from the means **1031** is further provided to the common file **105** via reading means **1024** and a line **107**. The common file **105** outputs public information X_A from a position indicated by this ID_A and this public information X_A, accompanied by ID_A in the reading means **1024**, is given to the cipher-key generating means **1023**.

The cipher-key generating means **1023**, using constants n and t from constant holding means **1021** and secret information r_B from secret information holding means **1028** for B besides these information pieces X_A and ID_A, generates a cipher-key K_B in accordance with:

$$K_B = (X_A^t \cdot ID_A)^{r_B} \bmod n$$

Therefore, key distribution can be achieved if the cipher-key K_A generated by the cipher-key K_A generating means **1019** of the subsystem **101** and the cipher-key K_B generated by the cipher-key K_B generating means **1023** of the subsystem **102** become identical because:

$$K_A = \alpha^{r_B \cdot t \cdot r_A} \bmod n = K_B$$

Thus, where both the sending party A and the receiving party B access the common file **105**, the subsystem **101** can achieve key distribution merely by adding its own identifying information ID_A to the ciphered message without having to prepare or transmitting a key distribution code.

Next will be described in detail, with reference to FIG. 6, a fourth preferred embodiment of the invention, in which both the first subsystem **101** and the second subsystem access the common file **105**.

It is supposed that, in this fourth preferred embodiment, a sending party A and a receiving party B access the common file **105**, and that, at the key distribution center **100**, a conversion formula and a common parameter are set as shown in FIG. 1. Referring to FIG. 6, identifying information for the receiving party B is entered from input means **1017**. In response to this input, common file reading means **1018** reads out public information U_B, V_B on B from a position indicated by ID_B in the common file **105**.

Verifying means **1010** checks whether or not $V_BU_B^{f\cdot(^{U}B,\ ^{ID}B)}$ is equal to ^{ID}B(mod n).

If the verifying means **1010** verifies the equality, it sends an OK signal to cipher-key generating means **1019**.

Cipher-key generating means **1019**, using secret information r_A from secret information holding means **1012** for A and a constant n from constant holding means **1013**, generates a cipher key K_A in accordance with:

$$K_A=U_B^{r_A} \bmod n$$

Here, $K_A=\alpha^{r_B t\cdot r_A}$ mod n because $U_B=\alpha^{r_B\cdot t\cdot r_A}$(mod n).

Identifying information ID_A from identifying information ID_A holding means **1015** for A is supplied to receiving means **1031** of the subsystem **102** via transmitting means **1008** and a line **104**. The information ID_A supplied from the means **1031** is further provided to the common file **105** via reading means **1024** and a line **107**. The common file **105** outputs public information U_A, V_A from a position indicated by this ID_A and public information U_A, V_A, accompanied by ID_A in the reading means **1024**, is given to the verifying means **1040**.

Verifying means **1040** checks whether or not $V_A^{t}/U_A^{f(^{U}A,\ ^{ID}A)}$ is equal to ID_A mod n.

If the verifying means **1040** verifies the equality, it sends an OK signal to cipher-key generating means **1023**.

The cipher-key generating means **1041**, using information U_A, a constant n from constant holding means **1021** and secret information r_B from secret information holding means **1028** for B generates a cipher-key K_B in accordance with:

$$K_B=U_A^{r_B} \bmod n$$

Therefore, key distribution can be achieved if the cipher-key K_A generated by the cipher-key generating means **1019** of the subsystem **101** and the cipher-key K_B generated by the cipher-key generating means **1023** of the subsystem **102** become identical because:

$$K_A=\alpha^{r_B\cdot t\cdot r_A} \bmod n=K_B$$

Next will be described in detail, with reference to FIGS. 7 and 8, a fifth preferred embodiment of the invention.

It is supposed that, at the key distribution center **100**, a conversion formula, a common parameter and secret information S_0 are set as shown in FIG. 1.

After the preparatory steps shown in FIG. 1, preparations particularly for the fifth embodiment are accomplished as described below.

Referring to FIG. 7, identifying information for a receiving party B, with whom a sending party A frequently communicates, is entered from input means **1017**. In response to this input, common file reading means **1018** reads out public information X_B on B from a position indicated by ID_B in the common file **105**.

X_B' generating means **1032**, using X_B from reading means **1018** and constants n and t from the constant holding means **1009**, converts the public information X_B into an easier-to-handle form in accordance with:

$$X_B'=X_B^{t}\cdot ID_B \bmod n$$

and stores X_B' into the ID_B address in a personal file **140**.

Next will be described the fifth preferred embodiment of the invention in further detail with reference to FIG. **8**.

Referring to FIG. **8**, receiving party identifying information input means **1017** enters receiving party identifying information ID_B. Then judging means **1033** judges whether or not the converted public information X_B' has been stored into the personal file **140**. In response to an affirmative judgment, personal file reading means **1034** provides ID_B to read the public information X_B' out of the personal file **140**. Cipher-key generating means **1035**, using a random number r from random number generating means **1011**, generates a cipher-key in accordance with:

$$K_A'=(X_B')^{r} \bmod n$$

If the judgment by the judging means **1033** is negative, the subsystem **101** obtains public information X_B for the receiving party B from the common file **105** with the common file reading means **1018** as well as externally provided identifying information ID_B for the receiving party B with the input means 1017. The random number generating means **1011** generates the random number r. Cipher-key generating means **1019**, using the public information X_B and the identifying information ID_B from the reading means **1018**, the random number r from the generating means **1011**, and constants n and t from constant holding means **1013**, generates a cipher-key K_A in accordance with:

$$K_A=(X_B^{t}\cdot ID_B)^{r} \bmod n$$

Both the cipher-key generated by the generating means **1035** and that by the generating means **1019** are K_A. $=\alpha^{r_B tr}$ mod n. Key distributing code Y_A generating means **1014**, after reading out secret information S_A from secret information holding means **1012** for A and the constants n and α from the constant holding means **1013**, uses said random number r to generate a key distributing code Y_A in accordance with:

$$Y_A=S_A\cdot\alpha^{r} \pmod n$$

The code Y_A generated by the generating means **1014** and the identify information ID_A for A are sent out to the line **104** by transmitting means **1016**. Code Y_A receiving means **1022** of the subsystem **102** receives the code Y_A and the identifying information ID_A for A, both provided via the line **104**. Using the identifying information ID_A and the code Y_A from the receiving means **1022**, the constants t and n from the constant holding means **1021**, and secret information r_B from secret information holding means **1028** for the receiving party B, generating means **1023** generates a cipher-key K_B in accordance with:

$$K_B=(Y_A^{t}\cdot ID_A)^{r_B} \pmod N$$

Here, $K_B=\alpha^{r_B tr}$ (mod n)

Therefore, key distribution can be achieved because the cipher-key K_A generated by the cipher-key generating means **1019** and **1035** of the subsystem **101** and the cipher-key K_B generated by the cipher-key generating means **1023** of the subsystem **102** become identical.

Next will be described in detail, with reference to FIGS. **9** and **10**, a sixth preferred embodiment of the invention.

First it is supposed that, at the key distribution center **100**, a conversion formula, a common parameter and secret information S_o are set as shown in FIG. **1**.

Preparations for the sixth embodiment are accomplished as described below.

Referring to FIG. **9**, identifying information for a receiving party B, with whom a sending party A frequently communicates, is entered from input means **1017**. In response to this input, common file reading means **1018** reads out public information U_B, V_B on B from a position indicated by ID_B in the common file **105**.

Verifying means **1010** checks whether or not $V_B^t/U_B^{f(U_B, ID_B)}$ is equal to ID_B (mod N).

If the verifying means **1010** verifies the equality, it stores the public information U_B into the ID_B address of the personal file **140**.

Next will be described the sixth preferred embodiment of the invention in further detail with reference to FIG. **10**.

Referring to FIG. **10**, receiving party identifying information input means **1017** enters receiving party identifying information ID_B. Then judging means **1033** judges whether or not the public information U_B has been stored into the personal file **140**. In response to an affirmative judgment, personal file reading means **1034** provides ID_B to read the converted public information U_B out of the personal file **140**. If the judgment by the judging means **1033** is negative, common file reading means **1018** reads public information U_B, V_B for B out of a position indicated by ID_B in the common file **105**.

Verifying means **1010** checks whether or not $V_B^t/U_B^{f(U_B, ID_B)}$ is equal to ID_B (mod n).

If the verifying means **1010** verifies the equality, it supplies an OK signal to cipher-key generating means **1035**.

The cipher-key generating means **1035**, using the random number from the random number generating means **1011**, generates a cipher-key in accordance with:

$$K_A=(U_B)^r \bmod n$$

Key distributing code Z_A, W_A generating means **1014**, using the random number r from the random number generating means **1011**, the secret information S_A from secret information holding means **1012**, the function f and the constants n, α and t from the constant holding means **1013**, generates key distributing codes Z_A and W_A in accordance with:

$$Z_A=\alpha^{tr} \pmod N$$

$$W_A=S_A\cdot\alpha^{r\cdot f(Z_A, ID_A)} \pmod n$$

The codes Z_A and W_A generated by this generating means **1014** and the identifying information ID_A from holding means **1015** are sent out by transmitting means **1016**. The information ID_A and the codes Z_A and W_A transmitted via a line **104** are received by receiving means **1030** of the second subsystem **102** and, at the same time, provided to verifying means **1024**.

Verifying means **1024**, using the information ID_A, the codes Z_A and W_A, and the function f and constants n

and t from holding means **1021**, checks whether or not $W_A/Z_A^{f(Z_A, ID_A)}$ is equal to ID_A (mod n).

If the verifying means **1024** verifies the equality, it supplies an OK signal to cipher-key generating means **1023**.

In response to this signal, the cipher-key generating means **1024**, using r_B from holding means **1028**, generates a cipher-key in accordance with:

$$K_B=Z_A^{\gamma B} \pmod n$$

Here, $K_B=\alpha^{trr}$ B (mod n)

Key distribution is made possible because $K_B=\alpha^{trr}$B (mod n)$=K_A$.

The fifth and sixth preferred embodiments of the invention are characterized by the presence of the personal file **140** on the first subsystem **101** side. In this file **140** are stored such pieces of information as are frequently used for communication by the first subsystem **101**. Other constituent elements of these embodiments are identical with the corresponding ones of the first through fourth embodiments. This personal file **140** contributes to reducing the amount of calculations in the fifth embodiment when generating a key for the other party with whom communication frequently takes place. In the sixth embodiment, it makes possible dispensation with the verifying means for public information on the other party with whom communication frequently takes place.

An example of the subsystems **101** and **102** for use in the first through sixth preferred embodiments will be described below with reference to FIG. **11**.

Referring to FIG. **11**, this system comprises a terminal unit (TMU) **301**, which may be a personal computer or the like having a function to process communications; a read only memory (ROM) **302**; a random access memory (RAM) **303**; a random number generator (RNG) **304**; a signal processor (SP) **306**; and a common bus **305** to connect the TMU **301**, ROM **302**, RAM **303**, RNG **304** and SP **306** with one another.

The RNG **304** may consist of, for instance, the key source **25** disclosed in the U.S. Pat. No. 4,200,700. The SP **306** may be composed of, for instance, a CY1024 Key Management Processor available from CYLINK.

The RNG **304** generates random numbers r upon an instruction from the SP **306**. In the ROM **502** are stored public integers t, α, n and one-way function f together with a secret integer S_A, γ_A (for use with the subsystem **101**) or γ_B (for use with the subsystem **102**). S_A, γ_A and γ_B may as well be stored by the user from his TMU into the RAM upon each occasion of communication. The above described actions are realized in accordance with a program stored in the ROM. The RAM **303** is used for temporarily storing the interim results of calculation or the like during the execution of these steps.

Each of the subsystems **101** and **102** may be a data processor of a general-purpose computer or an IC card.

As hitherto described in detail, the present invention provides the benefit of making possible safe unidirectional key distribution immune from attempts in collusion at illegitimate alteration of information..

While this invention has thus been described in conjunction with the preferred embodiments thereof, it will now readily be possible for those skilled in the art to put this invention into practice in various other manners.

What is claimed is:

1. A cipher-key distribution system for distributing a cipher key for use in cipher communication by a first communicating party with a second communicating party, provided with:

a common file for storing public information in a position indicated by receiving party identifying information, and first and second subsystems, wherein:

said first subsystem comprises:

reading means for reading said public information out of said common file;

random number generating means for generating random numbers;

first cipher-key generating means for generating a cipher key based on a constant, said receiving party identifying information, a random number generated by said random number generating means and the public information read out by said reading means;

first secret information holding means for holding a first secret information of said first communicating party using said first subsystem, said first secret information not accessible to said second communicating party;

key distributing code generating means for generating a key distributing code based on said constant, said random number and the first secret information given from said first secret information holding means; and

transmitting means for transmitting the key distributing code generated by the key distributing code generating means and information for identifying the first communicating party, and

said second subsystem comprises:

receiving means for receiving the key distributing code and the information for identifying the first communicating party from said transmitting means of the first subsystem;

constant holding means for holding the constant;

second secret information holding means for holding the second secret information of said second communicating party using said second subsystem, said second secret information accessible only to said second communicating party; and

second cipher-key generating means for generating a cipher key, which is identical with the cipher-key generated by said first cipher-key generating means, based on the key distributing code and information for identifying the first communicating party from said receiving means, the constant from said constant holding means and the second secret information from said second secret information holding means.

2. A cipher-key distribution system for distributing a cipher key for use in cipher communication by a first communicating party with a second communicating party, provided with:

common file means for storing public information in a position indicated by receiving party identifying information, and first and second subsystems, wherein:

said first subsystem comprises:

first reading means for reading said public information out of said common file means;

first secret information holding means for holding a first secret information of said first communication party using said first subsystem said first secret information not accessible to said second communicating party;

first cipher-key generating means for generating a cipher key based on a constant, receiving party identifying information, the public information read out by said first reading means and the first secret information from said first secret information holding means; and

transmitting means for transmitting information for identifying the first communicating party using this subsystem, and

said second subsystem comprises:

receiving means for receiving the information for identifying the first communicating party given from said transmitting means;

second reading means for reading said public information out of said common file means;

constant holding means for holding the constant;

second secret information holding means for holding the second secret information of said second communicating party using said second subsystem said second secret information accessible only to said second communicating party; and

second cipher-key generating means for generating a cipher key, which is identical with the cipher-key generated by said first cipher-key generating means, based on the constant from said constant holding means, the second secret information from said second secret information holding means, the public information given from said second reading means, and said information for identifying the first communicating party from said receiving means.

3. The cipher-key distribution system for distributing a cipher key for use in cipher communication by a first communicating party with a second communicating party, as claimed in claim 1, wherein the first subsystem further has a personal file for storing part of the public information stored in the common file.

4. The cipher-key distribution system for distributing a cipher key for use in cipher communication by a first communicating party with a second communicating party, as claimed in claims 1, 2 or 3, wherein the first subsystem further has verifying means for verifying the public information read out of the common file.

5. The cipher-key distribution system for distributing a cipher key for use in cipher communication by a first communicating party with a second communicating party, as claimed in claims 1 or 3, wherein the second subsystem further has verifying means for verifying the information received from said first subsystem.

* * * * *